Gruppo di Iniziativa Forense

Con il patrocinio dell'Ordine degli Avvocati di Verona
Con il patrocinio del Consiglio e Collegio Notarile di Verona

Incontro sul tema

Privacy e studi legali

Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico

Verona 27 febbraio 2004 ore 15,00

Sala Convegni UNICREDIT BANCA d'Impresa S.p.A. - Via Garibaldi n.2

Saluto del Presidente Ordine Avvocati di Verona
Saluto del Presidente Consiglio e Collegio Notarile di Verona

Introduce i lavori: Avv. Luca Venturini – Presidente G.I.F.

Internet, posta elettronica e privacy: esigenze di sicurezza e comportamenti a rischio: Dott. Gerardo Costabile - Guardia di Finanza di Milano - Member of "The International Association of Computer Investigative Specialists" (pagg. 2-8)

Prima interpretazione sugli aspetti penalistici della normativa: *Dott.* Aldo Celentano, Procura della Repubblica di Verona(in corso di pubblicazione)

Informativa e consenso del cliente: Avv. Marisa Bonanno, Foro di Verona (pagg. 9-23)

Le misure di sicurezza minime e idonee per gli strumenti elettronici: avv. Luca Giacopuzzi, Foro di Verona (pagg.24-30)

Le misure di sicurezza da adottarsi per il trattamento degli atti e documenti cartacei: Avv. Giulia Ferrarese, Foro di Verona(pagg.31-39)

Suggerimenti per la stesura del DPS da approntarsi entro il 31.3.2004: Avv. Antonio Francesco Rosa, Foro di Verona (pagg. 40-59)

Interventi:
Avv. Andrea Turco, Foro di Verona presenta una ***Proposta di documento per l'informativa e consenso negli studi legali*** (pagg.60-74)
Avv. Giannantonio Danieli, Foro di Verona: ***Privacy e deontologia*** (pagg. 75-83)

GRUPPO DI INIZIATIVA FORENSE

"Internet, posta elettronica e privacy: esigenze di sicurezza e comportamenti a rischio" (estratto dell'intervento di Gerardo Costabile – Iacis member - durante la conferenza a Verona del 27 febbraio 2004 – "Privacy e studi legali[1]")

Paradossalmente, lo scopo principale della mia presenza qui, non è quello di fornire risposte adeguate, ma far nascere dei dubbi, accrescere la consapevolezza che è necessaria una nuova mentalità per incrementare la sicurezza. Non c'è insicurezza maggiore che un presuntuoso senso di inviolabilità, oppure la sottovalutazione dei rischi, pensando di non essere un target appetibile o di non detenere dati particolarmente riservati.

Di contro, invece, la sicurezza è assimilabile ad un processo, non ad un prodotto. La forza della lunga *chain of security* sarà strettamente legata alla forza dell'anello più debole, che è quasi sempre l'uomo.

La nostra sicurezza e riservatezza sono strettamente ed indissolubilmente legate a quelle degli altri nostri interlocutori. Non è necessario un vero e proprio attacco informatico, ma sarebbe sufficiente un banalissimo virus informatico per compromettere la riservatezza di una confessione di un nostro amico ricevuta via posta elettronica. Peggio ancora se il computer fosse usato per attività professionali, dove il nostro Hard disk è di sovente lo scrigno di molti dati particolarmente riservati, stante anche il

[1] Durante la relazione sono stati effettuati due test "live": uno di fake mail con falso virus allegato (che ha dimostrato la facilità di invio di una mail a nome di un altro) e uno di recupero di un file riservato da un floppy ceduto ad un terzo, seppure formattato (per segnalare l'attenzione al punto 22 dell'allegato B del TU Privacy).

legame fiduciario del professionista con il proprio cliente.

Molte sono le sottovalutazioni, spesso giustificate da una scarsa informazione e da un basso livello di conoscenza dello strumento informatico e delle relative applicazioni. Anche un semplicissimo file di Office contiene molti dati, in funzione di quelli forniti durante l'installazione. Basta poco, anche un semplice salvataggio in altri formati, o l'utilizzo di apposite utility, per evitare ciò.
Un particolare riferimento, poi, ai programmi di *sharing* (tipo Kazaa, Winmx, Emule, etc.), dove in nome di una condivisione di gusti (spesso musicali) ci si ritrova a condividere –più o meno coscientemente- anche altre risorse, talvolta di natura professionale se il personal computer è utilizzato in maniera promiscua.

Il punto debole, quindi, con l'accrescere prepotente della tecnologia e della sicurezza dei sistemi, appare sempre di più quel "piccolo" uomo, schiacciato da sé stesso e dai suoi errori.
La tecnica utilizzata, perciò, per ingannare ed aggirare con la psicologia i processi di sicurezza, prende il nome di *"social engineering"*. L'ingegnere sociale è colui il quale, con particolare astuzia, riesce ad arrivare dove è difficilmente possibile con i normali strumenti di intrusione informatica, spingendo la vittima o un suo collaboratore, tramite espedienti principalmente psicologici, a rivelare informazioni apparentemente irrilevanti, ma che consentiranno un accesso abusivo, una frode o altre premeditate attività illecite (ad esempio inducendo l'utente ad autoinfettarsi con un trojan).
Le "tendenze base" della natura umana che vengono coinvolte in un tentativo di social engineering sono molteplici. Le più importanti, principalmente per le attività di diffusione dei virus, sono due: l'autorevolezza e l'ignoranza.
Per quanto concerne il primo aspetto sono numerosi i casi registrati in cui un semplicissimo messaggio di posta elettronica, ad esempio a nome di una software house oppure di un più "istituzionale" ufficio dell'FBI, abbia indotto l'utente ordinario, in

particolare soggezione psicologica, ad installare un allegato infetto, ad esempio indicato come un nuovo aggiornamento del programma. In questi casi è palese la tecnica di falsificazione del mittente del messaggio di posta elettronica sfruttando, comunque, anche la seconda "debolezza": l'ignoranza. Infatti l'impossibilità di conoscere ogni recondita tecnica informatica ed ogni angolo della rete Internet, consente all'aggressore di confezionare con una certa facilità un messaggio apparentemente serio e affidabile, particolarmente tecnico nel lessico e quindi spesso incomprensibile, nonché efficace.

Il rischio più elevato per la riservatezza e per l'integrità dei nostri dati è proprio la subdola "infezione virale": l'attacco dei "Malware". La parola "Malware" deriva dalla fusione di "Malicious" e "Software". Questa macrocategoria racchiude le famiglie di Virus veri e propri, Worm e Trojan.

Le "antologie informatiche" forniscono numerose definizioni, più o meno appropriate, del fenomeno e delle terminologie utilizzate. La definizione che desidero invece utilizzare è quella del Codice Penale, perché poi è in tale ambito che ci si dovrà confrontare nel caso di abusi. Il malware è "un programma informatico... omissis..., avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi un esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".

Il canale di infezione più utilizzato e quindi più "remunerativo" è la posta elettronica, che registra anche un forte incremento nell'ultimo anno 2003.

Tra i programmi della stessa macroarea si segnala anche il "Trojan Horse" (ovvero il c.d. "Cavallo di Troia") il quale, nascosto in un apparente innocuo programma o una fotografia, consente all'untore di controllare o registrare informazioni della vittima operando direttamente sull'hard disk di quest'ultimo a distanza. I Trojan vengono

generalmente riconosciuti sia dagli antivirus che dai firewall[2], anche se vengono utilizzate speciali utility ad esempio per inglobare il virus in coda al programma originale oppure nascondendo le estensioni dei file. In pratica il file "caio.jpg.exe" (in realtà un eseguibile), verrà visualizzato come un più innocuo "caio.jpg" (un formato per le fotografie digitali), ma con un'icona tipica dei programmi eseguibili.

Lo scopo è molteplice: potrebbero interessare file dati (comuni, personali, sensibili, giudiziari), fotografie, numeri di carte di credito, password d'accesso, documenti personali. Un altro motivo spesso riscontrato è quello di creare una macchina "zombie", pronta ad obbedire ai comandi dell'attaccante e quindi sferrare ulteriori attività delittuose ai danni di terzi, che "leggeranno" l'azione come proveniente dalla vittima del Trojan e non dal reale attaccante.

E' palese che, anche se l'attività fosse frutto di un gioco, come spesso accade, il sistema risulterebbe evidentemente vulnerabile ad eventuali successivi attacchi di reali malintenzionati.

Nelle aziende e negli studi professionali l'approccio al problema della proporzionalità tra uso della posta elettronica ed esigenze di sicurezza informatica è fortemente dibattuto.

Certamente l'importante è una buona policy, da rispettare a partire dalle funzioni apicali della struttura interna, dove siano definite regole e responsabilità. Sarà necessario proteggere il sistema informatico interno da virus che possano compromettere l'intera rete dello studio, guardando oltre i 6 mesi (quasi ridicoli) dell'imposizione ex lege. Dovranno essere protetti i dati e informazioni confidenziali, più che i singoli personal computer: evoluzione, peraltro, che la stessa legge ha fatto dal '96 ad oggi. Il costo che si può pagare è molto alto, non solo per le sanzioni, ma per i danni economici, le responsabilità ex art. 2050 cc, le conseguenti perdite di immagine e reputazione.

---

[2] **Firewall**: "muro di fuoco". Meccanismo HW e/o SW che permette di impostare restrizioni all'accesso ad uno o più computer collegati in rete. In genere rappresenta l'insieme delle misure di sicurezza a protezione dei dati fra la Rete (aziendale o esterna) e un calcolatore.

A questo punto vi lascio con una provocazione: ma è davvero indispensabile il "Documento programmatico della sicurezza"? E' davvero necessaria una imposizione ex lege, che peraltro non è nuova ma risale al 1999?

Vademecum per la sicurezza dei personal computer

a cura di Gerardo Costabile - gerardo@costabile.net

1. La sicurezza totale non esiste: informatevi, tenetevi aggiornati, prevenite.

2. Attivate la password di BIOS[3] e la password dello *screen saver*, al fine di evitare che altre persone possano accedere al computer e carpirne i dati durante la vostra assenza.

3. Modificate periodicamente le password ed evitate di affidare a Windows la memorizzazione automatica delle stesse (posta elettronica, accesso remoto, etc.). Tutte le password gestite direttamente dal sistema operativo Windows **sono altamente insicure**. E' consigliabile digitare la password ogni volta che questi servizi vengono utilizzati.

4. Considerate il PC come un **oggetto personale sia in azienda che in casa**, alla stregua di carte di credito, carta d'identità, ecc. Non consentitene l'utilizzo a chiunque e, nel caso di problemi hardware o software che comportino la necessità di interventi, preferite sempre l'assistenza qualificata.

5. Attuate sempre una valida **protezione hardware** di base, ponendo una o più etichette adesive autografate sulle viti posteriori del cabinet (la stessa tecnica attuata da molte case produttrici per controllare l'invalidazione delle garanzie).

6. Evitate di usare la connessione internet con un PC contenente dati riservati e/o personali. Se è inevitabile la connessione, durante le **navigazioni** attivate sempre un **firewall**[4] (locale o di rete) e mantenete attivo in background un **antivirus costantemente aggiornato**. Impostate i livelli di sensibilità e di protezione al massimo.

[3] Il BIOS (o SETUP) è un insieme di istruzioni con cui il computer ha la possibilità di riconoscere l'hardware installato nella macchina; esso è fisicamente residente all'interno di un chip della scheda madre detto ***Flash rom*** del Bios.

[4] Letteralmente significa "muro di fuoco" ed effettivamente è un sistema progettato per arginare l'accesso ai dati, impedendo, ad esempio, agli utenti provenienti da Internet, l'accesso non autorizzato ad una Intranet, cioè una rete privata. Può essere realizzato sia via software sia hardware ed è composto da un router che analizza i dati entranti e uscenti dalla rete privata.

7. Eseguite la **criptazione di tutti i files** riservati o particolarmente delicati utilizzando chiavi non banali di lunghezza min. 8 caratteri alfanumerici e, normalmente, non presenti nei vocabolari in nessuna lingua (es. "**32y47f_lvj"**). Evitare assolutamente chiavi "brevi" e/o riferite a parole presenti nei vocabolari, come ad esempio "**sole**" o "**computer**", nomi propri, date di nascita, ecc. Eventualmente dotatevi di un programma di crittografia (es. PGP). Molti sono freeware, liberamente scaricabili da internet, e, spesso, si trovano anche nei CD delle riviste specializzate del settore. La maggior parte di essi permette anche funzioni di cifratura della posta elettronica e di firma digitale.

8. Evitate assolutamente comportamenti a rischio **durante la navigazione in Internet**; Internet è probabilmente la più potente risorsa multimediale a disposizione dell'umanità, ma l'approccio ad esso deve essere governato da conoscenza, moderazione e prudenza di fondo.

Sono comportamenti a rischio:

- **la navigazione** su siti di Hacking, cracking, ecc, senza apposite protezioni;
- **scaricare software** da siti poco attendibili o non ufficiali;
- aprire **messaggi di posta elettronica** e eseguire **files allegati** ai messaggi senza preventiva scansione antivirus (anzi, prima si dovrebbe effettuare l'aggiornamento e poi si dovrebbe aprire il programma di posta elettronica);
- installare programmi scaricati da siti **non ufficiali** o comunque di natura incerta;
- dar credito a un messaggio pubblicitario dalle caratteristiche sospette (spesso di natura erotica o che promette facili guadagni) **che reindirizza ad un sito internet** "per saperne di più";
- tenete sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla vostra macchina. Disattivate sul browser l'esecuzione automatica degli script Java e ActiveX;
- mentre navigate prima di selezionare un link, posizionateci sopra il cursore del mouse e osservatene il percorso sulla apposita barra del browser: se è un file eseguibile probabilmente è un trucco per scaricarvi un dialer o peggio;
- evitare di inviare posta elettronica in formato "html" che, seppure consente una forma più elegante e/o simpatica, è uno dei metodi più subdoli per veicolare contenuti virus, worm e frodi (**senza necessità di allegati)**.

9. Eseguite periodicamente la **pulizia del disco da cookies, file temporanei, etc.** e, successivamente, cancellate gli stessi definitivamente con programmi specifici.

10. Ricorrete possibilmente alle versioni più recenti del sistema operativo e dei programmi maggiormente utilizzati, con particolare riferimento agli applicativi che consentono l'accesso ad internet.

11. Testate periodicamente il vostro PC per verificarne il livello di sicurezza, mediante importanti siti internet specializzati.

12. Non rispondete ai messaggi di posta "non sollecitati", chiedendo di essere cancellati da quella lista di invio: in tal modo rischiate di fare il gioco di chi li ha spediti, facendogli capire che la vostra casella di posta è attiva.

13. Non comunicate la vostra mail a siti ai quali non siete veramente interessati e/o sui quali avete anche il minimo dubbio.

14. Evitate i falsi allarmi e le catene di S. Antonio, controllando preventivamente la bontà delle informazioni prima di girarle (ad esempio grazie a siti specializzati come http://www.attivissimo.info/antibufala/elenco.htm).

GRUPPO DI INIZIATIVA FORENSE

Con il patrocinio dell'Ordine degli Avvocati di Verona

Con il patrocinio del Consiglio e Collegio Notarile di Verona

Incontro sul tema

Privacy e studi legali

Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico

Verona 27 febbraio 2004 ore 15,00

****

INFORMATIVA E CONSENSO DEL CLIENTE

Avv. Marisa Bonanno – foro di Verona

Fra le regole generali per il trattamento dei dati personali il nuovo Codice (art.13 D.lgs 196/2003) disciplina forma e contenuto dell'**informativa** che il titolare del trattamento (il professionista) deve fornire all'interessato (il cliente).

Fra le regole ulteriori, specifiche per privati ed enti pubblici economici, è inserito **il consenso al trattamento dei dati** (artt. 23 e ss.). Nello stesso capo III del titolo III sono contenute particolari garanzie per il trattamento di dati sensibili e dati giudiziari (artt. 26 e 27).

I due adempimenti sono strettamente connessi e complementari.

Premessa:

E' da rilevare, per quanto riguarda i signori **Notai** presenti oggi, che quanto diremo su informativa e consenso riguarda la componente strettamente "professionale" della loro attività, quella **"qualificata consulenza legale super partes"** che il Notaio fornisce al

proprio cliente, spesso anche contestualmente all'espletamento della propria competenza funzionale pubblica. Quest'ultima invece esimerebbe di per sè il Notaio dall'obbligo di raccogliere il consenso al trattamento ed è regolata dal capo II del titolo III, sul quale non possiamo in questa sede soffermarci.

D'altra parte, la ricorrente compresenza di due funzioni si ritrova anche nelle attività di assistenza e patrocinio svolte dall'avvocato negli incarichi giudiziali, laddove il difensore, libero professionista, può sicuramente qualificarsi "privato" ai sensi della legge sulla privacy, anche se in concreto l'esercizio del servizio di pubblica necessità, comporta alcune particolari esenzioni.

Di queste duplici funzioni dovremo necessariamente tenere conto nel valutare l'opportunità di adottare le garanzie più complete, a tutela dei nostri rispettivi clienti.

Ma prima di vedere in dettaglio in cosa consistono gli obblighi di informativa e consenso, cerchiamo di puntualizzarne la terminologia essenziale. Ciò ci sarà indispensabile per capire *“chi debba informare chi e di che cosa ”* (che sarebbe già un passo avanti!) ma anche per assumere la giusta posizione relazionale con la **ratio della normativa**: *Il trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. (art.2).*

In sostanza dovremmo forse abituarci a parlare più propriamente e significativamente di **“protezione” dei dati personali**, anziché semplicemente di privacy, che di per sé, non esprime nessuno dei valori sopra enunciati: è meno di riservatezza, meno di identità o personalità….

Quando un cliente si affida ad un professionista subito viene a porre nella sua sfera di conoscenza e nella sua disponibilità una serie di dati personali. E' importante quindi focalizzare per prima cosa **le definizioni normative**, che offre l'art.4. In particolare:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la

selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

L'elencazione è data in un crescendo di importanza e di esigenza di protezione, dalla semplice raccolta alla diffusione (che significa comunicazione a un numero indeterminato di destinatari), e contiene una precisazione importante e nuova rispetto alla precedente formulazione della 675/96: il trattamento non presuppone necessariamente la registrazione del dato in una **banca dati**.

Raccomandiamo inoltre un'attenta lettura delle definizioni di dato personale, identificativo, sensibile, giudiziario.

Tengo a richiamare alla vostra attenzione la netta differenza fra la nozione di dato giudiziario e quella di dato personale (comune, identificativo, sensibile, giudiziario) trattati in sede giudiziaria, su cui avremo modo di ritornare.

Ciò posto, è evidente che il professionista che riceve i dati personali del **cliente** ne assume le relative responsabilità ed in quanto tale gli incombono, fra i primi, gli obblighi di informativa e di consenso.

Ma chiediamoci preliminarmente: qual è la posizione dell'avvocato nei confronti dei dati personali di **persone diverse dal cliente** (la controparte, i testimoni, altri terzi) di cui venga a conoscenza nell'espletamento del mandato? E' possibile che in quanto non direttamente titolari del relativo trattamento o perchè non raccolti presso il nostro studio non abbiamo alcun obbligo nei confronti di detti dati?

In realtà essi sono comunque salvaguardati dai principi generali del codice e in particolare dall'art.1 secondo cui *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."*

Ritengo inoltre che in alcune ipotesi particolari il legislatore si riferisca (in modo implicito ed incidentale) al dato personale della controparte (es: art.26 comma 4 lett.c) ultimo inciso).

L'autorizzazione generale del Garante per i dati sensibili, cui torneremo ad accennare, prevede che 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, e sempre nel rispetto dei **principi di proporzionalità, determinatezza dell'incarico e legalità**. L'autorizzazione al trattamento dei dati giudiziari prevede invece che se i dati sono raccolti **per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive**, 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.

Vorrei poter ritenere che tali specifiche salvaguardie debbano ritenersi estensibili a tutti i dati di "terzi" rispetto al rapporto professionale di mandato.

L'Informativa:

Perché allora il cliente deve essere "informato"? Una risposta già di per sé convincente potrebbe essere questa: perché l'art.161 del codice prevede per la **violazione *dell'art.13*** *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.*

Restano salve eventuali ulteriori responsabilità anche penali per il trattamento illecito (es.: mancata o illegittima raccolta del consenso al trattamento) nelle specifiche ipotesi previste dall'art.167.

Dobbiamo ricordare poi che l'art.15 prevede l'applicabilità dell'art.2050 cod.civ. oltre che la risarcibilità del **danno non patrimoniale** arrecato per effetto del trattamento illecito di dati personali e ciò anche nel caso di violazione dell'art.11 (modalità di trattamento). Si tratta di una responsabilità aggravata che può essere evitata dal titolare soltanto dimostrando, di avere adottato le "misure idonee ad evitare il danno"; ma in tema di misure preventive (tali possono considerarsi, con interpretazione "estensiva", anche i doveri di informativa e consenso)……se le misure fossero state idonee, per definizione il danno non si sarebbe verificato! E' quindi evidente che si potrebbe ottenere l'esonero

da responsabilità unicamente provando un caso fortuito o la sussistenza di una causa di forza maggiore.
L'argomento verrà ripreso nella relazione relativa alle misure di sicurezza, propriamente dette.

Queste sanzioni che abbiamo enunciato sono certo ragioni molto “forti” per occuparci di informativa e consenso, ma non è questa la giusta chiave di lettura. In realtà l’informativa 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. Per questo motivo essa deve essere chiara ed il più possibile analitica. L'invalidità dell'informativa inoltre compromette la validità del consenso al trattamento, come vedremo.

Veniamo quindi all’art.13, dal quale estrapoliamo le prescrizioni più importanti dando la precedenza ai contenuti sulle forme.

L’informativa deve essere resa **sempre** dal professionista, anche per la forma minima di trattamento-dati: la raccolta, quindi indipendentemente dal fatto che detti dati verranno poi gestiti, registrati o consultati per il tramite di strumenti informatici o anche solo cartacei ed indipendentemente dall'utilizzo di banche dati.

Essa deve essere resa dal o dagli avvocati-**titolari** personalmente anche nel caso di associazione professionale, stante la personalità e fiduciarietà del mandato e quindi del conferimento dei dati stessi, oltre che in ottemperanza al tenore letterale della definizione normativa "anche unitamente ad altro titolare". E’ opportuno tuttavia che si faccia menzione della struttura organizzativa dello studio.

Deve essere prestata all'interessato, oppure alla persona presso cui i dati vengono raccolti (es.: il rappresentante legale o volontario del medesimo).

Deve contenere inoltre i nominativi di tutti i componenti dello studio, abituali sostituti d’udienza, praticanti ed altri ausiliari dello studio (personale di segreteria, amministrativo e/o contabile e fiscale) nella qualità di **incaricati** del trattamento, nonchè del

responsabile del trattamento, figura eletta facoltativamente, di cui si avrà occasione di parlare in tema di documento programmatico e di misure di sicurezza.

Devono essere chiaramente indicati, fra l'altro, le **finalità e modalità** del trattamento, laddove si dovrà avere ben presente anche il disposto dell'art.11 sulle modalità di trattamento e sui requisiti dei dati, che devono essere:

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Tutto quanto precede andrà specificamente segnalato in ordine alle **singole tipologie di dati** (comuni, identificativi, sensibili o giudiziari) in questione.

Dovrà esplicitarsi, per quanto possa sembrare ultroneo, che tali dati verranno indicati negli atti di causa o nella corrispondenza nei confronti delle **controparti, terzi intervenuti, testimoni e dei pubblici uffici**, costituendo anche questa una forma di "comunicazione", il tutto per le finalità inerenti l'espletamento del mandato e nei precisi limiti spaziali e temporali strettamente necessari, in relazione alla singola tipologia; lo stesso dicasi per eventuali, ma improbabili, esigenze di "diffusione" a terzi.

Si indicherà inoltre la **natura obbligatoria o facoltativa** del conferimento dei dati, con le conseguenze di un eventuale rifiuto di fornirli (mentre il rifiuto di prestare il consenso al trattamento andrà valutato in relazione alla specifica obbligatorietà del medesimo, in considerazione dei doveri professionali di prestare il patrocinio e di portare a termine l'incarico giudiziale).

Quando deve essere resa l'informativa? Come regola generale 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.

Può ritenersi, ma la disposizione non è chiara sul punto, che debba ricomprendervisi una specifica esenzione dall'obbligo di informare del trattamento la controparte processuale e gli altri interessati che non hanno direttamente conferito i propri dati al titolare del trattamento (es. testimoni).

La forma con cui viene resa l'informativa non deve essere necessariamente scritta, ma visto che si potrebbe porre un problema di prova e che comunque, a quanto vedremo, sarà talvolta opportuno procurarci il consenso (espresso e/o scritto) al trattamento ed infine per il semplice fatto che una forma più rigorosa comporta una maggiore attenzione per il contenuto dell'atto da parte di chi ne è destinatario, è altamente consigliabile che sia **redatta per iscritto.**

E' consigliabile infine che il testo dell'informativa sia il più ampio, dettagliato e chiaro possibile, come vedremo dall'esempio pratico che ci offrirà il collega Turco.

Il Consenso:

Per tutti i privati e per gli enti pubblici economici il consenso dell'interessato ad ogni tipo di trattamento dati deve essere **espresso e documentato in forma scritta** per i dati comuni, **espresso in forma scritta** per i dati sensibili, **specifico** per l'intero trattamento ovvero una o più operazioni dello stesso, comunque chiaramente individuati. **E' valido solo in presenza di valida informativa.**

Oltre ai settori specifici di cui al capo II, **si è esentati dall'obbligo di ottenere il consenso**, per quanto ci occupa in questa sede: quando è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; quando riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la

normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati; quando riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale; quando è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo; quando è prestato in vece dell'interessato per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato; quando è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; in altri casi specificamente individuati per provvedimento del Garante e comunque poco ricorrenti nella nostra professione.

Quanto abbiamo appena detto **non vale per i dati sensibili e per quelli giudiziari**, per i quali valgono altre, più restrittive esenzioni individuate negli artt.26 e 27 e per i quali, anche quando non è necessario il consenso, rimane ferma l'obbligatorietà dell'autorizzazione del Garante. I dati idonei a rivelare lo **stato di salute** non possono mai essere "diffusi" senza consenso scritto. Nella maggior parte dei casi sopra detti non è ammessa la "comunicazione" dei dati senza consenso.

Per i **dati sensibili** segnaliamo in particolare che il consenso non è necessario quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto 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**.

Per il trattamento dei **dati giudiziari** il consenso dell'interessato non è previsto.

Per i **dati comuni** quindi, secondo una diffusa interpretazione, il professionista sarebbe prevalentemente esente dall'obbligo di consenso in quanto agisce per definizione

nell’esecuzione di un contratto di mandato in cui il cliente è parte o per adempiere ad un obbligo precontrattuale su sua specifica richiesta.

Il consenso non sarebbe poi necessario, come abbiamo detto, **per il tempo strettamente necessario a far valere o difendere un diritto in sede giudiziaria**.

Sappiamo bene tuttavia che nella maggior parte dei casi le cose non sono così semplici.
Il mandato professionale di cui siamo investiti comporta un’ampia discrezionalità operativa e per quanto possiamo essere fedeli e rispettosi del dovere deontologico-professionale di informazione del cliente, spesso questi non è in grado o non si cura di seguire scrupolosamente le singole attività e le scelte difensive che poniamo in essere.
Non è neppure sempre facile valutare, al momento di conferimento di un incarico, se una vertenza troverà sicuro sfogo giudiziale e quanti e quali altre specifiche informazioni relative alla persona verremo a raccogliere nello svolgimento dell'incarico.

Con riferimento alla **conservazione** dei dati personali (art.16), ed in particolare per quelli **utilizzati in sede giudiziaria**, soprattutto se di natura sensibile, si pone il problema della durata del diritto del professionista alla conservazione, dopo l'esaurimento dell'incarico. Ritengo che il diritto alla conservazione, da esplicitarsi nell'informativa e nella dichiarazione di consenso, debba rapportarsi al periodo di durata dell'obbligo di rendiconto del mandatario (art.1713 cod. civ.) e della relativa prescrizione decennale, restando ininfluente la prescrizione presuntiva di cui all'art. 2961 c. c. (Cass. civ., 7 giugno 1991, n. 6461); il tutto nel rispetto ovviamente dei principi sopradetti di non eccedenza e determinatezza. L'autorizzazione generale n.7/2002 prevede inoltre che "Al fine di assicurare che i dati siano strettamente pertinenti e non eccedenti rispetto alle finalità medesime, i soggetti autorizzati valutano specificamente il rapporto tra i dati e i singoli obblighi, compiti e prestazioni".
Nel dubbio, sarà opportuno, anche sul punto, procurarsi il preventivo consenso informato dell'assistito.

Per i dati comuni e con riferimento all'**attività personale ed alla corrispondenza** del professionista ricordo che l'art.16 prevede per la cessazione del trattamento che i dati siano conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione.

****

E’ pertanto consigliabile munirci della **forma più ampia e rigoristica** di consenso dell’interessato, che non deve voler dire, guardate bene: il più generica possibile, perché verremmo così a contravvenire all’obbligo di specificità ed individualità del consenso.

E visto che in ogni caso consenso ed informativa sono indissolubilmente connessi è opportuno che vengano redatti **in unico corpo**, non importa in quale ordine, purchè **causalmente connessi**, in modo che sia chiaro che il consenso prestato si riferisca alle tipologie, modalità e finalità di trattamento specificamente enunciate nell’informativa, di cui contestualmente l'interessato **accusa ricevuta**.

La forma sarà quella **scritta** (la più rigorosa prevista per i dati sensibili), con le ordinarie cautele che adottiamo nella redazione di una scrittura privata e quindi senza spazi bianchi, abrasioni o cancellature. Data e firma saranno chiaramente apposte in calce e a margine di ogni mezzo foglio, in forma leggibile, dall'interessato. E’ naturalmente opportuno che al cliente venga **rilasciata una copia fotostatica del documento**.

****

Ma non basta. Oltre all'obbligo generale di informativa ed al consenso che abbiamo inquadrato e descritto, per due particolari categorie di dati sussiste un ulteriore onere: **l'autorizzazione**. L'art.26 del TU recita: *1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.*

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare e prosegue formulando una serie di eccezioni su cui non ci possiamo soffermare.

Rileva il fatto che per i **dati sensibili**, cioè quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico

o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, come abbiamo visto, **il consenso è (quasi) sempre obbligatorio ed oltre all'informativa occorrerebbe anche l'autorizzazione del Garante.**

L'art. 27, invece, con riferimento ai dati giudiziari, recita: *1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.*

Per nostra fortuna il Garante ci è venuto in soccorso con due **autorizzazioni generali**, rispettivamente relative al trattamento dei dati sensibili e di quelli giudiziari, sulle quali non ci è possibile soffermarci di più: sono le autorizzazioni nn. 4 e 7, pubblicate nell'anno 2002 e rinnovate nel giugno scorso, con le quali i liberi professionisti, ivi esplicitamente inclusi gli avvocati, i loro praticanti e incaricati e tutti "i liberi professionisti tenuti ad iscriversi in albi o elenchi per l'esercizio di un'attività professionale", **sono permanentemente autorizzati al trattamento dei dati sensibili (e giudiziari) dei loro clienti.** L'autorizzazione n.4 precisa alcune particolarità in ordine a finalità e modalità dei trattamento, richiamando fra l'altro l'obbligo permanente di informativa e di consenso scritto dell'interessato. Se i dati sono raccolti **per l'esercizio di un diritto in sede giudiziaria o per le indagini difensive**, 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.

****

In definitiva possiamo già andare traendo le prime **conclusioni**: informativa e consenso sono obblighi di legge nella maggior parte dei casi; rincorrere le maglie del codice per evitarli, ove si possa, non avrebbe senso: è importante acquisire invece **un elevato grado di attenzione per la protezione del dato personale che ci consenta di fornire un'informativa il più ampia, completa e comprensibile per l'interessato**. Ciò anche in considerazione delle peculiarità del mandato professionale e soprattutto delle diverse tipologie di servizi legali prestati dai nostri studi; ripeto che, almeno la grossa fetta di noi civilisti, sa bene che quando riceviamo un incarico non sappiamo mai in anticipo: se

la questione troverà sfogo giudiziale o no; quanti e quali interessati potranno inserirvisi, quali terzi, quali tipologie di dati potremo incontrare cammin facendo e così via, l'adozione della forma più ampia dettagliata e "protettiva" si impone. **Un documento unico quindi, comprensivo di consenso al trattamento e informativa, costruito con il massimo formalismo richiesto, che non si limiti a riportare le norme di legge in modo anonimo ed aspecifico, ma determinato e proporzionato, in senso spaziale e temporale, agli usi professionali.**

****

Concludo, se ho ancora cinque minuti, con **uno sguardo al web**.

Chi di Voi si è attrezzato con **sito web informativo delle attività professionali** e soprattutto se per mezzo di internet intende fornire servizi professionali on-line, nei limiti di cui al nuovo art.17 Codice Deontologico Forense e dell'art.10 Dlgs. n.70/2003 attuativo della direttiva europea sulla società dell'informazione (2000/31/CE), come pure servirsi della posta elettronica per rapporti professionali con clienti e colleghi, oltre a tutti gli obblighi in tema di misure di sicurezza, non solo a tutela del trattamento dei dati personali, ma dei nostri sistemi informativi in genere, dovrà pure tenere presente che secondo le ampie definizioni di dato personale e identificativo: *(b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;)* anche il trattamento di un indirizzo di posta elettronica del tipo marisa.bonanno@studiumfori.it (contenente quindi nome, cognome e dominio registrato a nome dell'interessato) è soggetto alla normativa che stiamo illustrando, e quindi quantomeno all'obbligo di informativa.

I colleghi responsabili di un sito web che vogliano raccogliere detti dati al fine della **distribuzione di una news letter o di una circolare informativa** sulle attività dello studio predispongano pertanto idonea informativa relativa allo specifico e limitato trattamento in questione, con espressa esclusione di ogni altro, indicazione del titolare responsabile e delle modalità di "cancellazione" dal servizio.

Ritengo che per tali attività il consenso non sia necessario ai sensi dell'art.24 lett.b): *"per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato".*

Diverso è il caso in cui il professionista intenda raccogliere altri dati personali per l'esercizio di servizi professionali on-line (sempre nei limiti consentiti dalla normativa civilistica e deontologica sopra richiamata): la cd "**consulenza on-line".** In questi casi la necessaria e/o opportuna prestazione del consenso informato al trattamento da parte dell'interessato potrebbe riproporsi negli esatti termini e limiti più sopra trattati.

Occorre avere ben presente in proposito che al fine della documentazione per iscritto del consenso o della sua espressione in forma scritta nel caso di dati sensibili, si renderà necessario che il consenso venga espresso formalmente e non solo “spuntato” in area non protetta, o trasmesso per e-mail semplice, per così dire "in chiaro", poiché ai sensi dell’art.10 DPR 445/2000 (cd TUDA) solo la firma elettronica, quantomeno "leggera", assicura il requisito di forma scritta, previsto dall'art.24, testè citato, mentre il meccanismo del cd "point and click" in un'area web accessibile al pubblico (e quindi con connessione non protetta) non sarebbe sufficiente.

Per un'attenta disamina delle problematiche connesse alla fase di acquisizione del consenso nella fase di registrazione dell'utente e successive, segnalo un chiaro articolo degli Avvocati Andrea Lisi e M. De Giorgi del Foro di Lecce, disponibile on-line sulla rivista Diritto & Diritti che tutti conosciamo, all'indirizzo web: http://www.diritto.it/articoli/dir_privacy/lisi_degiorgi.html , nonché la recente pubblicazione per i tipi della Simone "La privacy in internet" sempre a cura del Collega Lisi.

Segnalo infine brevemente, a titolo di curiosità, che con un recente parere (newsletter N. 194 del 1 - 7 dicembre 2003 che potete consultare sul sito del Garante) l’Autorità Garante ha autorizzato, definendo limiti e garanzie, **una importante casa editrice a trattare dati sensibili** relativi anche a opinioni politiche, sindacali, religiose, appartenenza etnica delle persone che richiedono **servizi di consulenza on line**, offerti a pagamento dalla stessa società attraverso siti e pagine web di testate giornalistiche. Medici, avvocati, psicologi, ed altri professionisti potranno rispondere a richieste formulate anche per e-mail, ma nel rispetto di determinate regole: i dati dovranno

essere pertinenti in rapporto all'argomento trattato o al quesito posto, oltre che indispensabili per fornire il servizio di consulenza on line. Alla società è stato, quindi, prescritto di inserire in modo visibile nell'informativa fornita agli utenti, l'invito a non indicare nei quesiti dati di carattere sensibile non strettamente necessari per la risposta. I quesiti verrebbero inviati agli esperti comunque privi dei dati anagrafici e indirizzi e-mail e le risposte arriverebbero automaticamente ai richiedenti attraverso dei codici identificativi, tramite il sistema informativo.

Nel caso poi che la domanda e la risposta dovessero essere inserite, previo consenso dell'utente, negli spazi consultabili liberamente dal pubblico (ad esempio in una rubrica delle domande più frequenti, faq), la società dovrà altresì verificare prima della loro pubblicazione che, oltre al nome e all'indirizzo e-mail dell'interessato, non vi siano altri dati, anche diversi da quelli sensibili, che possano rendere identificabile l'interessato. La società dovrà, inoltre, impartire agli esperti (che vengono designati responsabili del trattamento) precise istruzioni per la verifica della pertinenza ed effettiva necessità dei dati sensibili riportati nei quesiti, ma anche per la loro eliminazione nel caso non fossero necessari. Gli "esperti on line" dovranno anche controllare che nelle risposte pubblicate non vi sia nessun elemento che permetta di risalire all'identità della persona che ha richiesto la consulenza.

E' quindi probabile che analoga autorizzazione verrebbe fornita, su richiesta e a pari condizioni, anche nell'ipotesi di **rubriche gestite direttamente da avvocati sui propri siti professionali**.

Mi permetto tuttavia di dubitare che tali rubriche e queste forme di consulenza spersonalizzata ed esposta al pubblico, possano ritenersi compatibili con il più specifico dovere di riservatezza e segreto imposto all'Avvocato dall'art.9 CDF, comprensivo di "tutte le informazioni" comunque fornite dal cliente, anche indipendentemente dalla realizzabilità in concreto della "non identificabilità" dell'interessato.

Avendo a disposizione ben altri esperti di deontologia, io ho finito e Vi ringrazio per l'attenzione.

Avv. Marisa Bonanno – Foro di Verona

Via San Leonardo, 4
Verona
Tel. 0458344304
Email: studiobonanno@studiumfori.it
www.studiumfori.it

GRUPPO DI INIZIATIVA FORENSE

Incontro sul tema

Privacy e studi legali

LE MISURE DI SICUREZZA MINIME E IDONEE PER GLI STRUMENTI ELETTRONICI

di

Avv. Luca Giacopuzzi del Foro di Verona – www.lucagiacopuzzi.it

SOMMARIO: 1) considerazioni introduttive - 2) le misure minime - 3) le misure idonee - 4) conclusioni

1) CONSIDERAZIONI INTRODUTTIVE

Albert Einstein ebbe modo di affermare che "l'uomo e la sua sicurezza devono costituire la prima preoccupazione di ogni avventura tecnologica". Evidentemente il grande scienziato non aveva in mente né computers né reti telematiche. Eppure il monito poc'anzi citato è quanto mai attuale!

D'altronde, oggi tutti utilizzano - o, per lo meno, conoscono - Internet.

L'impatto tecnologico sulla vita sociale ed economica non è oggetto di scelte, ma è inevitabile, nel bene e nel male. Limitarsi soltanto a subire questo radicale ed ineluttabile processo di trasformazione della società corrisponde all'incapacità di coglierne compiutamente gli aspetti vantaggiosi, che sono molti.

In questo senso la scelta fra essere produttori o consumatori di tecnologia non è libera o opzionale. Chi non investe in sviluppo tecnologico con tutta probabilità sceglie una via non solo di declino economico, ma anche sociale e culturale.

E', insomma, un dato di fatto – oltre che un dato di comune esperienza – che dall'impiego delle tecnologie tutti noi non possiamo (più) prescindere, pena una irreversibile perdità di competitività, un gap che poi sarebbe molto difficile colmare.

Ecco spiegato, dunque, perché dobbiamo confrontarci con la sicurezza informatica, dato che le nuove tecnologie - oltre ai benefici, straordinari, che esse portano agli utenti – spesso racchiudono in sé potenziali pericoli per i dati personali e la riservatezza della vita privata dei fruitori delle tecnologie stesse.

2) LE MISURE MINIME

Esaurita questa doverosa premessa, di carattere introduttivo, addentriamoci in un contesto più strettamente giuridico ed osserviamo, da subito, che il Testo Unico sulla privacy affronta il tema della sicurezza al Titolo V della Parte Prima.
Due, in particolare, le misure di sicurezza che vengono in rilievo: quelle c.d."minime" e quelle c.d."idonee".

Le prime, previste in via generale dagli artt.33 e ss. T.U., sono in concreto individuate dal disciplinare tecnico di cui al c.d."allegato B" (che sostituisce il sistema delle "misure minime" del d.P.R. 318/99, ora abrogato, emanato in attuazione dell'art.15 della L.675/96) e sono volte ad assicurare un livello (appunto) minimo di protezione dei dati personali. Un livello al di sotto del quale non si può scendere: il mancato rispetto di dette misure, infatti, ai sensi dell'art. 169 T.U. costituisce reato, punito con l'arresto fino a 2 anni o con l'ammenda da 10.000 a 50.000 Euro.

Le misure minime si suddividono in 2 categorie, a seconda che il trattamento dei dati personali avvenga "con" o "senza" strumenti elettronici.

Per quanto concerne la prima ipotesi, va rilevato che l'art. 34 T.U. elenca ben otto misure minime. Nell'individuazione di esse, alcuni concetti ricorrono più di altri.

Sotto questo profilo, pare così opportuno segnalare la particolare attenzione che il Legislatore riserva alla nozione di "autenticazione informatica" (art.34, lett.a): la definizione è nuova (ossia sconosciuta alla L.675/96) e comprende i mezzi – siano essi programmi informatici o componenti hardware – deputati alla verifica ed alla convalidazione dell'identità di un dato soggetto.

E'una misura di particolare importanza, dato che essa, se correttamente posta in essere, garantisce il controllo di chi accede agli elaboratori. L'autenticazione informatica, infatti, ha il compito di verificare l'identità di chi andrà a trattare i dati personali, e di convalidarla dopo averla verificata.

Ciò è possibile grazie all'utilizzo delle c.d. "credenziali di autenticazione", prescritte alla successiva lettera b) del medesimo art. 34, le quali consistono in quei "dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica".

Al di là della definizione poc'anzi citata (art.4, comma 3, lett.d)), va detto – semplificando – che le moderne tecnologie informatiche, per il riconoscimento dell'identità, adoperano i tradizionali codici di accesso e le parole chiave oppure altri dispositivi non mnemonici, i quali ultimi, peraltro, già oggi sono largamente utilizzati.

Nella moderna accezione del controllo degli accessi, pertanto, le credenziali sono costituite da qualcosa che il soggetto incaricato "conosce" (ad esempio: un codice identificativo o una parola chiave), "possiede" (ad esempio: una smart card, un token), oppure "è" (ad esempio: una caratteristica biometrica, come l'impronta di un dito, del volto, della retina).

Al punto 3 del Disciplinare Tecnico è espressamente previsto che ad ogni incaricato siano assegnate o associate individualmente una o più credenziali per l'autenticazione. I termini "assegnate" o "associate" sono relativi alla differenza tra le diverse tipologie di credenziali: una password può essere assegnata, ma non altrettanto un tratto biometrico, che è già patrimonio esclusivo dell'individuo e per queste credenziali è dunque riservato il concetto di associazione e non di assegnazione.

Data la particolare delicatezza che rivestono, le credenziali devono essere custodite gelosamente, come si preoccupa di ricordare il punto 4 del Disciplinare.

La credenziale ad oggi più utilizzata è la parola chiave. A nessuno, infatti, sfugge il significato della c.d. "password", stringa di caratteri alfanumerici, liberamente scelta da un dato soggetto, e ad esso associata.

Nonostante il fatto che essa, in concreto, possa contenere ogni segno presente sulla tastiera di un PC, variamente unito ad altro significante, la casistica insegna che l'utente del sistema, quando viene lasciato libero di scegliere la propria parola chiave, di fatto tenderà a sceglierne una facile da ricordare, come il nome di un familiare.

Ecco, quindi, che la Legge si premura di specificare in uno specifico punto (il 5) le caratteristiche che deve avere una password per essere realmente tale. Sono così prescritte regole di composizione e di uso, che garantiscono un livello di sicurezza minimo.

A norma del Disciplinare Tecnico, infatti, la parola-chiave dovrà essere 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, inoltre, non dovrà contenere riferimenti agevolmente riconducibili all'interessato (es.: nome della moglie, marca dell'autovettura, squadra di calcio della quale si è tifosi, ecc.) e sarà modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi, che diventano tre in caso di trattamento avente ad oggetto dati sensibili o giudiziari.

Le combinazioni basate su credenziali esclusivamente mnemoniche sono però in genere meno sicure delle altre. Ciò spiega il favore sempre crescente delle credenziali c.d. biometriche, all'opposto considerate le più affidabili. Il Garante della Privacy, chiamato a pronunciarsi sul punto, è in ogni caso intervenuto con un provvedimento dettato dalla prudenza (newsletter n. 182 dell'8-14 settembre 2003), secondo il quale l'utilizzo generalizzato ed indiscriminato di tali sistemi non è consentito in quanto esso viola il principio di proporzionalità tra gli strumenti impiegati e le finalità prospettate.

Successivamente al riconoscimento (e, quindi, successivamente all'identificazione) dell'incaricato, un "sistema di autorizzazione" (altra misura "minima", contemplata all'art. 34 lett.c)) permetterà al soggetto, verificato attraverso le credenziali ad esso associate, di trattare i dati.

E'necessario, a tal fine, che l'incaricato sia stato previamente autorizzato dal titolare (o, se designato, dal responsabile) a trattare determinati dati, ai sensi dell'art. 30 del Codice. Si tratta, non è chi non veda, di un adempimento preliminare di particolare importanza, che deve essere effettuato per iscritto, con una puntuale specificazione dell'ambito del trattamento consentito.
L'individuazione dei singoli trattamenti consentiti (ad un soggetto, ad esempio, sarà permesso unicamente prendere visione dei dati, e non anche cancellarli o modificarli; un altro incaricato, invece, potrà aver accesso solo ai dati comuni, e non anche a quelli sensibili, ecc.) andrà a costituire il c.d. "profilo di autorizzazione" del singolo incaricato, profilo che sarà sottoposto a verfica almeno una volta all'anno (Punto 14 D.T.).

Correlata alla misura poc'anzi esaminata è, in un certo senso, quella prevista alla lettera successiva del medesimo art. 34, la lettera d).
Questa misura di sicurezza è finalizzata ad una periodica revisione delle autorizzazioni per il trattamento dei dati, nonché delle operazioni consentite agli addetti alla manutenzione ed agli addetti alla gestione degli strumenti hardware e software. La lista degli incaricati ed i relativi profili di autorizzazione – viene precisato al punto 15 del Disciplinare – può essere redatta anche per classi omogenee di incarico.

Particolarmente significativa, poi, è l'indicazione contenuta alla lettera e) dell'art 34.
La norma, che prescrive la protezione degli strumenti elettronici e dei dati da accessi non consentiti e programmi maligni, tende ad impedire che i dati siano trattati

illecitamente (ossia in spregio delle prescrizioni di legge), che si verifichino accessi non consentiti nonché azioni distruttive causate da virus, worm e, in generale, da ogni altro codice pericoloso per l'integrità e la confidenzialità del dato stesso.

Sotto questo profilo è importante notare che ogni accesso al sistema informatico compiuto da soggetti non autorizzati è considerato "accesso abusivo". Detta violazione, perciò, potrà essere posta in essere non solo da persone estranee all'impresa/studio professionale (come, ad esempio, un hacker), ma anche – e più frequentemente – dai dipendenti stessi, che accedono a determinati dati per i quali non possiedono profilo di autorizzazione e di incarico.

Evidentemente, capire come avviene un attacco è di fondamentale importanza per prevenire l'attacco stesso. Non è questa la sede per una disamina, seppur frettolosa, dell'argomento. Basti sul punto sapere che l'attacco viene di norma preceduto da alcune azioni "preparatorie", articolate in 2 componenti: la prima comportamentale, la seconda tecnica.

La parte comportamentale si avvale di tecniche operative definite di "ingegneria sociale" (social engineering) e di fatto consiste nel reperire informazioni sul bersaglio da colpire sfruttando la naturale propensione delle persone a rispondere a domande dirette ed impreviste, ad aiutare qualcuno che sembra in difficoltà o, all'opposto, che ricopre una carica di prestigio.

La seconda componente, di natura prettamente tecnica, viene invece detta di "ricerca dell'impronta" (footprint). L'hacker, prima di sferrare l'attacco al target, deve infatti raccogliere le necessarie informazioni sull'architettura del sistema, ed in particolare sulla protezione della struttura.

I soggetti che connettano il proprio sistema informatico alla rete Internet, quindi, devono proteggersi (in una rete ben protetta, infatti, solo le aggressioni più sofisticate – e quindi, statisticamente, le meno probabili – possono realmente mettere in crisi il sistema). Ecco, allora, che pare opportuno seguire la prescrizione contenuta al punto 20 del Disciplinare (il quale prescrive l'adozione di "idonei strumenti elettronici" a protezione dei dati sensibili o giudiziari dagli accessi abusivi) qualunque sia il tipo di dato personale oggetto di trattamento, e non solo – come invece prevede l'allegato B – quando venga in rilievo un dato classificato come sensibile o giudiziario. Come noto, il più diffuso strumento di difesa delle reti informatiche è chiamato firewall: dall'adozione di esso, pertanto, non si può prescindere, qualunque sia la grandezza e l'importanza dell'impresa/studio professionale da proteggere.

Per altro verso, giova osservare che gli attacchi sono favoriti, oltre che dalle possibili debolezze delle misure di sicurezza poste a protezione del sistema, anche dalle vulnerabità del software.
E'noto, infatti, che il software contiene molto spesso dei "bug" (letteralmente "insetto"), ossia delle imperfezioni. Alcune di esse sono innocue; altre, invece, facilitano gli attacchi informatici.
Consapevoli di ciò, pertanto, mano a mano che dette vulnerabilità vengono individuate, i produttori del software interessato rilasciano appositi programmi – detti patch ("pezza") - volti ad ovviare al malfunzionamento dell'applicativo stesso. Il punto 17 del D.T. ci ricorda che è buona norma ricercare frequentemente gli aggiornamenti dei programmi impiegati; detta operazione, in ogni caso, va effettuata almeno una volta all'anno.

Le misure di sicurezza non potevano escludere dall'ambito delle loro previsioni la criticità più ricorrente per i sistemi informatici, rappresentata dall'azione dei c.d. "virus" e loro derivati (script virus, stealth virus, worm, trojan horse), genericamente accomunati sotto l'etichetta di "malware", parola anglosassone derivante dalla crasi tra "malicious" e "software".

La “periodicità minima di aggiornamento” di programmi anti-virus (fissata dalla legge in sei mesi: cfr. punto 16 D.T.) è però motivo di ilarità, dato che – come noto a chiunque abbia un minimo di dimestichezza con apparecchiature informatiche – se un software antivirus non viene aggiornato almeno giornalmente esso non è realmente efficace.

Un’ulteriore disposizione, prevista alla lettera f) dell’art.34 e ripresa in dettaglio ai punti 18 e 23 del Disciplinate Tecnico, riguarda l’obbligatorietà di effettuare, almeno ogni settimana, copie di back-up dei dati contenuti nei propri sistemi informatici. Il precetto – non contempato dalla L.675/96 – è senza dubbio importante, ma, a ben guardare, la previsione di legge poc’anzi citata appare “monca”, dato che la stessa dimentica di abbinare alla procedura di “salvataggio dei dati” la non meno necessaria procedura di verifica del “restore” dei dati, al fine di salvaguardare l’effettività di un “disaster recovery”.

Non basta, infatti, effettuare copie di sicurezza, senza constatare periodicamente che il dato ivi contenuto sia realmente disponibile ed integro. Il processo di disaster recovery (ossia quel processo che consente di ripristinare il normale funzionamento del trattamento dei dati in seguito ad una inaspettata interruzione del trattamento stesso) va quindi sempre condotto, sebbene la legge ne prescriva l’obbligatorietà con riferimento ai soli trattamenti aventi ad oggetto dati sensibili o giudiziari.

Da ultimo, pare opportuno segnalare che è prevista quale “misura minima” anche la tenuta di un documento programmatico sulla sicurezza (c.d. DPS).

La predisposizione di un documento programmatico annuo sulla sicurezza è una misura già prevista dal d.P.R. 318/99, ma il Disciplinare Tecnico innova sensibilmente sul punto, dato che nel precedente decreto il DPS doveva essere obbligatoriamente stilato solo in caso di trattamento di dati sensibili e/o giudiziari effettuati mediante elaboratori accessibili in Rete.
Con l’impianto normativo attuale detto documento (che, in buona sostanza, è una rappresentazione puntuale dei rischi aziendali e delle contromisure da adottare per gestire l’eventuale emergenza) assume un’importanza fondamentale nella pianificazione di ogni scelta di sicurezza aziendale ed entra a far parte delle documentazioni “obbligatorie” che le imprese che trattano dati sensibili o giudiziari devono tenere. Per espressa disposizione di legge, infatti, il titolare deve riferire nella relazione accompagnatoria del bilancio d’esercizio dell’avvenuta redazione o aggiornamento (incombenza annuale:entro il 31 marzo) del DPS.

Volendo, a questo punto, tracciare un giudizio globale sugli adempimenti imposti, in tema di misure minime, al soggetto che tratti dati personali, va detto che l’adozione delle nuove misure potrebbe creare notevoli problemi applicativi a migliaia di studi professionali ed imprese medio-piccole, che non hanno alle proprie dipendenze persone con le necessarie competenze tecniche.

Il legislatore, in considerazione del fatto che i titolari potrebbero così assumere responsabilità per interventi esguiti da altri (segnatamente, da consulenti informatici) ha ritenuto opportuno tutelarli, prevedendo l’obbligo – al punto 25 D.T. - per l’installatore di rilasciare una “dichiarazione scritta” dell’intervento effettuato, che ne attesta la conformità alle disposizioni del D.T.

3) LE MISURE IDONEE

Prendendo ora in esame le misure c.d. “idonee”, va osservato che esse sono disciplinate dall’art. 31 T.U., articolo che impone al titolare del trattamento dei dati personali di predisporre tutte le misure di sicurezza idonee a ridurre al minimo “i rischi di

distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

A questo punto, un'importante osservazione: se l'adeguamento alle "misure minime" implica l'assenza di responsabilità penali, tale adeguamento non è sufficiente per affrancarsi da responsabilità civile qualora l'evoluzione tecnologica renda disponibili accorgimenti ulteriori che soddisfino le misure dichiarate "idonee".

Ciò perché – ai sensi dell'art. 15 T.U. – "chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.".
L'art. 2050 c.c., infatti, (norma alquanto rigorosa, dettata in tema di esercizio di attività pericolose) prevede che l'esercente l'attività pericolosa – e quindi, nel nostro caso, il titolare del trattamento - vada esente da responsabilità solo se riesca a dimostrare di aver adottato tutte le misure idonee ad evitare il danno. In caso contrario, ai sensi del 2°comma dell'art. 15 T.U., egli dovrà rispondere anche del danno non patrimoniale (come accaduto nel caso deciso dal Tribunale di Orvieto con sentenza 22.11.02 n. 254: fattispecie in tema di risarcimento dei danni morali sofferti da alcuni clienti di un Istituto bancario).

Come si evince facilmente, l'adeguamento alla previsione di legge poc'anzi citata (art. 2050 c.c.) è particolarmente difficoltoso. Secondo la giurisprudenza, infatti, può provare di aver adottato ogni misura idonea chi dimostri di aver rispettato "tutte le tecniche note" – anche solo astrattamente possibili – all'epoca del fatto (cfr. Tribunale di Milano, 19 novembre 1987, in Foro Italiano, 1988, I, 144).

Da altro punto di vista, è opportuno precisare che nell'ambito dei danni da risarcire non sarà incluso il solo pregiudizio patrimoniale (nelle note forme del "danno emergente" e "lucro cessante"), ma anche il danno morale, come si desume dall'inequivoco tenore dell'art.15 D.Lgs. 196/03.

L'espressa estensione al trattamento di dati personali della risarcibilità del danno non patrimoniale è sintomatica della particolare attenzione che il Legislatore ha voluto rivolgere ai danneggiati, dal momento che il danno che ricorre più frequentemente è proprio quello relativo alla sfera morale dell'individuo, di cui sarebbe stata altrimenti esclusa la risarcibilità (stante il precetto dell'art. 2059 c.c.).

Il titolare e il responsabile, perciò, oltre a quelle minime previste, devono anche adottare misure di prevenzione "idonee" a ridurre - per quanto possibile - i rischi, prevenibili e prevedibili, che incombono sui dati.

Riassumendo, l'impresa/lo studio professionale che operi on line, al fine di "ridurre i rischi", dovrà:
a) osservare il livello di sicurezza minimo di legge (per evitare conseguenze penali);
b) approntare le misure di sicurezza ulteriori, che in base al caso concreto si potevano predisporre (altrimenti dovrà risarcire i danni eventualmente cagionati a terzi).

4) CONCLUSIONI

Avviandoci a concludere, va notato che le sanzioni per chi ignori la legge ci sono, ed esse – specie in tema di omessa adozione delle misure minime – sono rigorose.

Mi sembra che già questo sia un motivo (un "buon"motivo) perché l'azienda/lo studio professionale prenda coscienza delle indicazioni di legge e vi si conformi.

I soggetti devono pertanto sì “proteggersi”, ma senza mai dimenticare che la sicurezza informatica sarà sempre una chimera finchè esisterà il fattore umano, l’anello più debole della catena.
Chiunque pensi che i prodotti da soli offrano “vera sicurezza” si sta cullando nella sua illusione.
La sicurezza non è un prodotto, ma un processo: è pertanto un’attività fatta di risorse e di persone, che riguarda la sfera organizzativa e non solo quella tecnica.

E’indubbio che tutto ciò richieda uno sforzo, che spesso viene visto con sfavore dagli operatori. Tuttavia credo che siano maturi i tempi perché l’azienda/ lo studio professionale possa capire che la tutela della sicurezza non è un valore antagonista alle esigenze di mercato.

La privacy, insomma, da “costo” deve essere vista come “risorsa”: è questo il salto culturale che oggi ci attende. La scommessa, in altre parole, è passare da un’interpretazione pedante e formalistica della privacy all’impostazione di una politica integrata in tema di sicurezza. E’ – credetemi – una scommessa vincente e, tra l’altro, molto remunerativa, dato che l’adottare politiche di riservatezza dei dati rappresenta un valore aggiunto al proprio prodotto o servizio. Una ragione in più, dunque, per adoperarsi in questo senso.

Avv. Luca Giacopuzzi
Corso Cavour 32
Verona
tel. 0458035655
email luca@lucagiacopuzzi.it

GRUPPO DI INIZIATIVA FORENSE

Incontro sul tema

Privacy e studi legali
Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico

Verona 27 febbraio 2004 ore 15,30

TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI
Relazione dell'avv. Giulia Ferrarese del Foro di Verona

Le operazioni di trattamento dei dati indicate dall'art. 4 D.Lgs. n. 196/03 ("operazioni… concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati") riguardano espressamente anche i trattamenti effettuati senza l'ausilio di strumenti elettronici.

Oggetto di trattamento sono i dati personali, cioè qualsiasi informazione su un soggetto (persona fisica o giuridica, anche non residenti). Ad esempio, sono dati personali i numeri di telefono abbinati al nominativo dell'intestatario, gli indirizzi e-mail se permettono di risalire al titolare.

Nell'ambito dei dati personali distinguiamo: dati sensibili, dati giudiziari e dati comuni.

Sono dati sensibili quelli che rivelano direttamente o che sono idonei a rivelare una informazione di tipo "sensibile" (tassativamente elencata nell'art. 4 lett. d) D.Lgs. n. 196/03).

Sono dati giudiziari quelli idonei a rivelare l'esistenza di provvedimenti tassativamente indicati nell'art. 3, comma 1, DPR n. 313/02 ovvero la qualità di imputato o di indagato.

Sono dati comuni i dati personali residuali, che non rientrano nei dati sensibili o giudiziari.

Le informazioni che integrano i dati personali possono essere veicolate non solo tramite la scrittura ma anche tramite le immagini (ad es. fotografie o riprese) od i suoni (ad es. la voce registrata nel corso di una telefonata).

Dati sensibili possono pertanto essere contenuti in documenti cartacei quali, ad esempio, le lettere, le cartelle cliniche ma anche nelle fotografie o nelle radiografie.

Le operazioni di trattamento, dettagliatamente descritte nell'art. 4 sopra riportato, si possono suddividere in tre categorie:

a) operazioni di raccolta dei dati (direttamente dall'interessato o da terzi);

b) operazioni di trattamento all'interno della struttura, per organizzare e rendere i dati agevolmente usufruibili (ad es. annotazione manuale in una rubrica di nomi, indirizzi e numeri di telefono; raccolta e conservazione dei dati nei fascicoli di studio, archiviazione dei fascicoli ovvero cancellazione o distruzione dei dati ad es. cestinando gli stessi);

c) uso dei dati nei rapporti con l'esterno:

- direttamente con il soggetto cui si riferiscono i dati raccolti;
- mettendo a disposizione di terzi i dati raccolti (comunicazione, diffusione) .

Oltre all'art. 4 cit., anche l'art. 11 D. Lgs. n. 196/03 detta regole valide anche per il trattamento dei dati senza l'ausilio di strumenti elettronici.

I dati vanno trattati:

- in modo lecito: cioè conformemente alle disposizioni del codice della privacy, nonché alle disposizioni del codice civile (il trattamento non deve pertanto essere contrario a norme imperative, all'ordine pubblico ed al buon costume);
- secondo correttezza: principio fondamentale che deve ispirare chi tratta qualcosa che appartiene alla sfera altrui;
- per scopi determinati (non è consentita la raccolta di dati come attività fine a se stessa), espliciti (il soggetto interessato va informato sulle finalità del trattamento), legittimi, compatibili con gli scopi per i quali sono raccolti (specialmente nella comunicazione e diffusione degli stessi);

- esatti (cioè precisi e rispondenti al vero) e, se necessario, aggiornati;
- pertinenti (in relazione all'attività che viene svolta), completi (non nel senso di raccogliere il maggior numero di informazioni possibili ma bensì di contemplare anche il rovescio della medaglia dei dati raccolti, con riferimento al concreto interesse e diritto del soggetto interessato), non eccedenti in senso quantitativo (onde evitare una sorta di "schedatura" del soggetto interessato);
- conservati limitatamente al periodo necessario in relazione agli scopi per i quali sono raccolti. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita (art. 25 D. Lgs. n. 196/03). Va tuttavia precisato che la norma deve essere coordinata con altre norme imperative: ad es. l'art. 2220 c.c. (che prevede che le fatture e la corrispondenza ricevuta nonché copia delle fatture e della corrispondenza spedita siano conservate per 10 anni), nonché l'art. 2961 c.c. (per cui ad es. gli avvocati sono esonerati dal rendere conto degli incartamenti relativi alle liti dopo tre anni da che queste sono state decise o sono altrimenti terminate e, trattandosi di prescrizione presuntiva, è altresì consigliabile conservare gli incartamenti, come è prassi, per dieci anni).

Se il trattamento di dati è effettuato in violazione di quanto disposto dal codice della privacy è necessario provvedere al "blocco" dei dati (sospensione temporanea di ogni operazione di trattamento) fino alla regolarizzazione del trattamento (ad es. fornendo l'informativa omessa o raccogliendo il consenso non dato) ovvero alla cancellazione dei dati se non è possibile regolarizzare. Per la violazione delle disposizioni in materia di trattamento sono previste sanzioni penali (art. 167, 2° comma).

L'art. 31 D.Lgs. n. 196/03 dispone che " i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Sono le c.d. misure idonee di sicurezza. Si tratta di accorgimenti che il soggetto che tratta i dati deve adottare per ridurre i rischi di:

- distruzione o perdita dei dati: ad es. a seguito di incendio;
- acceso non autorizzato ai dati: ad es. estranei che si introducano nei locali per rubare dati o farne copia ovvero dipendenti che accedano ai dati senza autorizzazione;
- trattamento non consentito o non conforme alle finalità della raccolta.

La norma non individua in concreto le misure minime che devono essere pertanto determinate dal titolare o dal responsabile.

Inoltre, la norma non parla di eliminazione totale dei rischi ma di riduzione degli stessi.

E' importante, pertanto, che se gli eventi negativi dovessero verificarsi (nonostante l'adozione delle misure) le conseguenze siano contenute grazie all'adozione di adeguati accorgimenti. Se ad es. estranei o ladri dovessero introdursi nei locali ove sono custoditi i dati (nonostante la presenza di un porta blindata) la conservazione dei dati sensibili in fascicoli inseriti in schedari chiusi (con la chiave non a portata) riduce il rischio di accesso a detti dati.

Le misure devono essere commisurate alla natura dei dati ed assicurare ad es. una maggiore protezione dei dati sensibili rispetto a quelli comuni.

Peraltro, se i dati sensibili e comuni sono trattati insieme e non è possibile separarli, sarà necessaria l'adozione delle misure di protezione più ampie.

Dette misure vanno poi aggiornate in relazione al progresso tecnico.

Il trattamento di dati effettuato "manualmente", cioè senza l'ausilio di strumenti elettronici, è disciplinato espressamente dall'art. 35 D.Lgs. n. 196/03 e dall'allegato B (disciplinate tecnico).

Possiamo individuare tre ordini di misure:

1) Redazione ed aggiornamento periodico del "mansionario privacy":

art. 35 lettera a)*: aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative*

allegato B punto 27: *Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*

E' pertanto necessario:

- almeno una volta all'anno, aggiornare il documento (c.d. mansionario privacy) contenente la definizione dei dati che gli incaricati sono autorizzati a trattare e la tipologia dei trattamenti consentiti. Il documento non va redatto personalmente per ogni incaricato ma si può redigere per classi omogenee di incarico, indicando altresì i nominativi degli incaricati che confluiscono nella medesima classe;
- vanno impartite istruzioni scritte agli incaricati per il controllo e la custodia degli atti e documenti durante tutto il ciclo delle operazioni di trattamento dei dati personali.

2) custodia di atti e documenti

art. 35 lettera b) *previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti*

allegato B punto 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.*

Collegando il disposto delle norme sopra indicate con l'art. 35 lett a) ed il punto 27 dell'allegato B) si deduce che gli atti e i documenti, contenenti dati personali, non devono essere lasciati vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre che gli incaricati, cui essi sono affidati per lo svolgimento delle loro mansioni, provvedano in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni loro affidate. Questa è una prescrizione di carattere generale, da ritenersi valida anche per gli atti ed i documenti contenenti solo dati di natura comune.

L'allegato B per gli atti e documenti contenenti dati sensibili e giudiziari prevede espressamente che gli incaricati provvedano a custodirli per tutto il tempo del trattamento ed a restituirli al termine delle operazioni di trattamento. Durante il trattamento atti e documenti non dovranno essere lasciati incustoditi ed è pertanto opportuno che gli incaricati siano dotati di cassetti con serratura ove riporre gli stessi se si allontanano anche temporaneamente ovvero al termine della giornata, qualora il trattamento non fosse terminato. Finito il trattamento i documenti dovranno essere restituiti ovvero ricollocati nel posto in cui sono stati prelevati (ad es. archivio o

schedario delle pratiche in corso). Non è pertanto necessario che il titolare o responsabile provveda a prelevare personalmente atti e documenti ed a consegnare gli stessi agli incaricati. E' sufficiente indicare all'incaricato quali atti e documenti trattare, lasciando a quest'ultimo il compito di prelevarli e riporli.

In definitiva, va prestata attenzione a che atti e documenti cartacei (anche lettere o comunicazioni pervenute tramite la posta o a mezzo telefax) od i fascicoli delle pratiche non si trovino sparsi sulle scrivanie (specie quando si ricevono clienti) o appoggiati su ripiani o in luoghi in cui siano visibili a terzi non autorizzati, che possono venirne a conoscenza e divulgarli. E' importante pertanto provvedere allo smistamento e consegna tempestiva al destinatario della posta e delle comunicazioni trasmesse a mezzo telefax, onde evitare che le comunicazioni rimangano incustodite e visibili a terzi. E' bene inoltre che i fascicoli siano custoditi negli appositi schedari (chiusi a chiave se nei fascicoli sono contenuti anche dati sensibili e giudiziari) e prelevati per il tempo necessario al trattamento. Sarebbe consigliabile quindi arrivare ad abituarsi a lavorare un fascicolo alla volta.

3) Archiviazione di atti e documenti

art. 35 lettera 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*

allegato B punto 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.*

Si precisa infine che il titolare, anche qualora vengano trattati dati sensibili (ad es. relativi La norma non detta più alcuna regola per l'archiviazione di atti e documenti contenenti solo dati di natura comune.

Per atti e documenti contenenti dati sensibili e giudiziari è invece implicitamente prescritta la conservazione in locali specifici a ciò destinati, che consentano il controllo nell'accesso.

E' prescritta l'adozione delle misure sotto indicate:

a) l'accesso agli archivi va controllato mediante uno dei seguenti accorgimenti:

- *strumenti elettronici (ad es. tesserino magnetico distribuito agli incaricati);*
- *incaricando alcune persone della vigilanza degli archivi;*
- *autorizzando preventivamente chi accede agli archivi (è consigliabile in tal caso tenere i locali destinati ad archivio chiusi a chiave e consegnare la chiave alla*

persona autorizzata con istruzioni di richiudere a chiave e restituire la chiave al termine delle operazioni);

b) *dopo l'orario di chiusura, le persone che accedono agli archivi vanno identificate e registrate;*

Le misure minime indicate nel disciplinare tecnico saranno aggiornate periodicamente in relazione all'evoluzione tecnica ed all'esperienza maturata (art. 36).alla salute dei dipendenti) solo su supporto cartaceo, è comunque tenuto ad accertarsi che il soggetto esterno cui sono trasmessi detti dati (ad es. chi è incaricato di elaborare le buste paga dei dipendenti) abbia adottato le misure minime previste a protezione.

Si allega un fac-simile di lettera di incarico al trattamento dei dati a personale dello studio e di lettera di incarico a terzi (ditta che effettua le pulizie dello studio).

E' opportuno segnalare che la normativa sulla privacy è entrata in vigore l'8.5.1997, il regime transitorio è oggi regolato dall'art. 180 e dall'art. 181 del Decreto L.gs. 30.6.2003 nr. 196.

Un ultima annotazione per i Notai, essi sono soggetti a precise regole di conservazione degli atti stabilite dalla Legge Notarile; valga per loro – come per tutti- il principio che se altre disposizioni stabiliscono regole, anche più rigide, per la conservazione ed il trattamento dei dati, in ogni caso sempre andranno salvaguardate ed assicurate le misura minime ed idonee introdotte con la col Dlgs 30.6.2003 nr. 196.

BOZZA DI LETTERA DI INCARICO AL TRATTAMENTO DEI DATI

Il sottoscritto ……in qualità di Titolare/Responsabile del trattamento dei dati dello Studio Legale……sito in……..

Incarica il Dr./sig./la sig.ra……nato/a a……il…….al trattamento dei dati personali nell'ambito delle funzioni di ….(ad es. segretaria)che è chiamato/a a svolgere.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato.

Premesso che:

- *il trattamento dei dati deve essere effettuato in modo lecito e corretto;*
- *i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;*
- *è necessaria la verifica costante dei dati ed il loro aggiornamento;*

- *è necessari ala verifica costante della completezza e pertinenza dei dati trattati;*
- *devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile e di cui al documento programmatico sulla sicurezza;*
- *in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:*

a) *divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;*

b) *l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;*

c) *la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso degli interessati rilasciato in forma scritta;*

- *in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;*
- *le proprie credenziali di autenticazione devono essere riservate.*

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Ciò premesso, nell'ambito della qualifica di……Le viene conferito l'incarico di compiere le operazioni di trattamento sotto elencate, con l'avvertimento che dovrà operare osservando le direttive del Titolare /Responsabile e nel rispetto dei principi di cui in premessa:

a) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

b) eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Pertanto potrà avere accesso a

Tutti i dati comuni, sensibili e giudiziari

Ovvero

Esclusivamente ai seguenti dati.....

Qualsiasi altra informazione può esserLe fornita dal Titolare che provvede anche alla formazione.

Per ogni altra misura ed istruzione qui non prevista ci si richiama al D.P.S., che viene allegato alla presente.

Verona, lì.... *Il Titolare del trattamento*

Per conoscenza ed accettazione

Avv. Giulia Ferrarese
Verona, via Rosa 8
Tel. 0458002239
Email rosa-ferrarese@iol.it

Bibliografia: "il nuovo codice privacy: che fare?" di M. Bernasconi e dr. M. L. Riva Diamind.com s.r.l.(scaricabile anche via internet) ed al quale ho fatto riferimento per le note di cui sopra.; "Guida pratica alle nuove misure di sicurezza per la privacy" F. Berghella . Maggioli Editore; Riem "Privacy e sicurezza", Edizione Simone.

GRUPPO DI INIZIATIVA FORENSE

CONVEGNO 27.02.2004

PRIVACY E STUDI LEGALI

RELAZIONE AVV. ANTONIO F. ROSA

L'art. 34 del D.Lgs. 30.06.2003 nr. 196 introduce, tra le misure minime, l'obbligo della tenuta del documento programmatico della sicurezza.

La stesura di un documento sulla sicurezza non è disposizione nuova, in quanto il precedente D.P.R. 318/1999 faceva pure riferimento all'obbligo di predisporre ed aggiornare, con cadenza annuale, un documento programmatico sulla sicurezza dei dati.

Al fine di disciplinare le misure di sicurezza, il precedente D.P.R. 318/1999 imponeva quest'obbligo a chiunque operasse il trattamento di dati sensibili e giudiziari mediante elaboratori elettronici accessibili in rete pubblica.

Tale normativa era stata interpretata nel senso che anche un singolo elaboratore connesso ad internet, o ad altri elaboratori mediante modem, dovesse essere considerato come accessibile mediante una rete di telecomunicazioni disponibili al pubblico.

Di conseguenza lo studio professionale che trattava dati sensibili e giudiziari mediante elaboratori connessi ad internet, era già soggetto all'obbligo della stesura di un documento sulla sicurezza ai sensi dell'art. 6 del D.P.R. 318/1999.

Oggi essendo venuta meno la distinzione tra elaboratori in rete accessibili al pubblico, o no, l'obbligo è previsto per tutti gli elaboratori (sia singolo, che in rete) che trattino dati personali di natura sensibile o giudiziaria.

E’ stata sollevata da qualcuno la questione se l’obbligo di stesura di un documento programmatico sulla sicurezza dei dati sussista anche per coloro che trattino con strumenti elettronici solo dati comuni, con esclusione quindi dei dati sensibili e giudiziari. Sostenere l’obbligatorietà anche in questo caso, significa andare contro il dato letterale della norma di riferimento, che non va individuata nell’art. 34, ma nel più specifico art. 19 dell’allegato B (disciplinare tecnico) del cosiddetto codice privacy.

Questa norma, inserita tra le misure da adottare in caso di trattamento con strumenti elettronici, disciplina la redazione del D.P.S.; esso indica chiaramente che si è obbligati alla stesura del documento solo in caso di trattamento di dati sensibili o di dati giudiziari. Questo è il dato letterale della norma: un’interpretazione estensiva della stessa, ai fini pubblicistici, non trova giustificazione né nella ratio legislativa attuale, né in quella precedente (ove lo scopo era chiaramente quello di provvedere alla tutela di questi dati dal pericolo di intrusione, manomissione o conoscenza da parte di terzi non autorizzati, dovuta all’esposizione in rete pubblica dell’elaboratore).

E’ però certamente consigliabile la stesura di un DPS anche in caso di trattamento di dati comuni con strumenti elettronici. Detta stesura risponde infatti 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 aziendale.

Quest’ultima considerazione ci porta ad esaminare qual è la ratio che sovrintende all’obbligo di provvedere alla stesura del DPS.

Lo scopo primario del DPS non è quello di controllo, come da taluno viene prospettato; il Garante, gli Organi accertatori non hanno certamente bisogno di un documento per verificare se la normativa è stata osservata. Nè la presenza del DPS è prova di aver rispettato in concreto le misure minime di sicurezza.

Limite che evidenzia come, a mio modesto avviso, il legislatore, imponendo la redazione e la tenuta del DPS tra le misure di sicurezza minime, ha avuto di mira, ancor prima della finalità di controllo, di perseguire la necessità che ogni titolare di

trattamento di dati, meritevoli, per la loro natura, di particolare tutela con strumenti elettronici (i più esposti), delinei a se stesso ed ai suoi incaricati il quadro delle misure di sicurezza adottate e da adottare sia sotto il profilo organizzativo che fisico e logistico e progetti un piano complessivo aziendale che riguardi la sicurezza di tutti i dati. Tant'è che il grado di rischio individuato nel DPS è destinato nel tempo a ridursi, man mano che si adottano nuove misure operative di sicurezza e si perfezioni il processo.

Questo progetto (o processo) sulla sicurezza dei dati corrisponde ad un ulteriore interesse del titolare, già obbligato deontologicamente alla riservatezza.

Da taluni viene contestato il fatto che la riservatezza aziendale o professionale era già di fatto assicurata come un valore assoluto preesistente. L'obiezione non ci sembra pertinente in quanto l'uso di strumenti elettronici ha insita la possibilità di perdite o alterazioni di dati indipendentemente dalla volontà del titolare stesso, anche solo per fatti involontari (si pensi alla perdita dei dati per un cattivo funzionamento del computer) o per i maggiori rischi collegati alla connessione all'esterno degli strumenti elettronici.

Concludendo, la stesura del DPS ha, per il titolare la preminente funzione di rispondere a precise norme di organizzazione aziendale, assicurando ai suoi clienti e fornitori la tutela dei dati. In quest'ottica andrà visto e steso; pur mantenendo nel contempo natura pubblicistica, perché imposto da una norma non derogabile, e posta a tutela di un diritto (tutela della privacy altrui) ritenuto dall'ordinamento di rango superiore. Nessun dubbio, pertanto, può sussistere sul fatto che l'omessa tenuta del DPS rientri tra le fattispecie di cui all'art. 169.

Per redigere il DPS si consiglia di procedere secondo il seguente iter organizzativo e processuale:

preliminare individuazione ed elencazione dei trattamenti di dati personali presenti nello studio;

analisi dei rischi che incombono sui dati;

stesura del mansionario;

L'individuazione e l'elenco dei trattamenti di dati personali Operativamente, per arrivare alla stesura di tale elenco bisognerà procedere individuando:

i tipi di dati personali che vengono trattati (per categorie);

gli strumenti che vengono utilizzati per il trattamento (anche in questo caso individuandoli per categoria).

Ad esempio in uno studio professionale (leggi il lavoro del Bernasconi) i tipi di dati personali che vengono trattati, in ordine tendenzialmente crescente di pericolosità per la privacy, sono:

- i dati comuni del personale e dei clienti, o di terzi ricavabili da fonti pubbliche (sono quelli meno pericolosi, perché per loro natura pubblici e detenuti legittimamente da terzi), ad esempio i dati camerali, quelli telefonici o di residenza tratti da elenchi consultabili liberamente;
- i dati comuni del personale dipendente o dei collaboratori, dei fornitori e dei clienti, o di terzi (sono i dati che vengono forniti previa informativa), ad esempio la P.IVA, la residenza, la data di nascita, il nr. di telefono cellulare, il numero di telefono non inserito in elenchi, gli indirizzi e-mail raccolti……..;
- i dati giudiziari del personale, dei fornitori e dei clienti;
- i dati sensibili del personale, dei fornitori e dei clienti, dei terzi (la casistica è vasta e variegata; ad esempio la condizione sociale, le prestazioni sociali ricevute, il reddito percepito o patrimonio posseduto, la sentenza applicativa di una pena su richiesta delle parti non rientrano nel trattamento severo riservato ai dati sensibili e giudiziari, in quanto dati comuni).

Individuare l'elenco dettagliato dei trattamenti è di fondamentale importanza per definire ed attuare le misure di sicurezza privacy, sulla base dell'analisi dei rischi. Infatti, esso potrebbe indurre il titolare anche a decidere di trattare i dati in modo diverso, rispetto a quanto fatto in precedenza. Tipico è l'esempio di chi decide di trattare dati sensibili con strumenti elettronici abbandonando una rete con connessione ad internet ed optando per il trattamento di tali dati solo tramite elaboratori che non sono in rete.

Individuati ed elencati i dati bisogna poi prendere in esame gli strumenti impiegati, anch'essi in ordine tendenzialmente crescente di pericolosità per la privacy, in relazione al più alto grado di violabilità dei dati che essi presentano, come segue:

schedari chiusi;

archivi chiusi;

computer non in rete in locali protetti;

computer non in rete in locali non protetti;

computer in rete senza accesso ad internet;

computer non in rete ma con accesso ad internet;

computer in rete e con accesso ad internet;

computer portatile con accesso ad internet o senza;

Aiuta certamente l'organizzazione il predisporre e tenere aggiornato un elenco di tutte le dotazioni hardware, software e di trasmissione dati, con le sostituzioni, riparazioni delle apparecchiature. Si avrà così una sempre aggiornata indicazione del sistema informatico e del suo stato.

Per ogni computer il rischio può essere verificato accedendo ad un sito di primaria casa di produzione di software di protezione e facendo testare il computer stesso, sarà possibile – spesso con molte sorprese- valutare in concreto il rischio per ogni singolo strumento elettronico.

L'analisi dei rischi

L'analisi dei rischi che incombono sui dati è il momento principale ed il fine da perseguire nella redazione del documento programmatico di sicurezza.

Il titolare dovrà individuare, dopo avere elencato i dati che tratta e gli strumenti che adopera per il trattamento, nel concreto quali sono i rischi specifici che potrebbero interessare i dati che tratta.

Pure se l'analisi impone la conoscenza di alcuni aspetti tecnici, essa è accessibile a chiunque e non necessariamente bisogna ricorrere all'ausilio di uno specialista

informatico. Molto poggia sul buon senso ispirato alla previsione, o meglio, prevedibilità dei rischi.

Se la logica dell'analisi è quella di prevedere i possibili rischi, la prima operazione da compiersi è quella di valutare le minacce che gravano sui singoli trattamenti di dati personali.

Per i vari tipi di dati andremo ad individuare il rischio che grava sul trattamento valutando la loro importanza in funzione della natura dei dati trattati.

Successivamente si potrà valutare le minacce che possono interessare gli strumenti (elettronici e non) impiegati per il loro trattamento.

Ad esempio, gli elaboratori elettronici possono, per la parte hardware degli strumenti, essere interessati da mal funzionamenti, dovuti a guasti causali o per difettosa manutenzione, corti circuiti, allagamenti e incendi, furti. Gli apparati di rete possono essere esposti a rischio di indebite intercettazioni o alterazioni della trasmissione di dati. I software ed i sistemi operativi possono essere stati progettati incompleti (le cd. falle informatiche) o installati non correttamente, erroneamente o dolosamente, consentendo ad utenti non autorizzati l'esecuzione di operazioni, oppure permettendo operazioni non autorizzate sul sistema o danneggiamenti al software (virus, i trojan horse) ovvero consentendo attacchi non distruttivi, il cui obiettivo è rendere il software inutilizzabile agli altri utenti del sistema. Le documentazioni cartacee sono minacciate dall'essere distrutte e/o alterate ad opera di eventi naturali, da azioni accidentali e di comportamenti intenzionali. I supporti di memorizzazione, su cui vengono tenute le copie dei software installati, dei file di log, dei back-up e dei dati personali, sono soggetti, oltre che ad alterazioni e distruzioni per eventi naturali, accidentali o di malintenzionati, anche al deterioramento o a difetti di costruzione che ne compromettono il funzionamento.

Ogni categoria di strumenti, suggerisce il Bernasconi, deve essere pertanto valutata e verrà espresso un giudizio riassuntivo sul grado di rischio cui sono sottoposti.

L’esperienza suggerisce che il grado di rischio maggiore va riconosciuto negli elaboratori che non sono in rete, specialmente se connessi ad internet, e primi tra tutti ai computer portatili.

Compiuta l’analisi che precede, si è in grado di valutare quali eventi negativi possono verificarsi nell’ambito dei singoli trattamenti e di identificare il grado di rischio da coprire, arrivando eventualmente a valutare l’opportunità di adottare ulteriori misure non necessarie ex lege, ma utili all’organizzazione per aumentare il grado di protezione dei dati.

L’individuazione dell’ambito di trattamento consentito agli incaricati, il cd. mansionario.

Per poter stendere il DPS bisogna avere individuato le figure del titolare, del responsabile, degli incaricati.

Con riferimento a questi ultimi bisogna individuare quali dati sono autorizzati a trattare.

Questa individuazione va fatta con un apposito documento, volgarmente detto mansionario, nel quale - con aggiornamento e verifica annuale- si identificano, per ogni singolo incaricato, le classi omogenee di dati che sono gli stessi autorizzati a trattare con o senza ausilio di strumenti elettronici, ed altresì chi sono gli addetti alla gestione e manutenzione degli strumenti elettronici e gli eventuali terzi autorizzati ad accedere agli studi.

La tenuta di questo documento è prevista dall’art. 35 della normativa e dagli art. 15 e 27 del disciplinare tecnico.

A questo punto necessita osservare come nel D.P.S. confluiscano tutti i documenti obbligatori che devono essere tenuti per la privacy. Abbiamo sopra fatto riferimento all’opportunità della stesura di un documento riguardante la raccolta degli interventi eseguiti sugli strumenti elettronici (non obbligatorio). Troviamo ora il cd. mansionario, vi troveremo anche il cd. Disaster Recovery, pure previsto dalla normativa come documento obbligatorio.

Elencati i trattamenti di dati personali, verificata l'analisi dei rischi che incombono sui dati trattati, individuate nel cd. mansionario le persone che trattano i dati, si può concretamente passare alla redazione del D.P.S.

La redazione del DPS

L'obbligo di tenuta del Documento programmatico è – come detto- previsto dall'art. 34 del D.Lgs. mentre il punto 19 del disciplinare tecnico individua chi deve redigerlo, i tempi ed il contenuto.

Appare opportuno segnalare ai Colleghi che hanno funzioni di Sindaco o sono componenti, nei limiti consentiti dagli ordinamenti professionali, di C.d.A. di società che il punto 26 del disciplinare tecnico impone, per i bilanci approvati successivamente al 1 gennaio 2004, l'obbligo, ovviamente se esistente, di attestare l'avvenuta redazione o aggiornamento del D.P.S.

Il Documento deve essere redatto ogni anno entro il 31 marzo, dal titolare del trattamento dei dati, anche attraverso il responsabile, se designato.

Deve avere la forma scritta e, ritengo, essendoci un termine, una data certa (suggerirei anche sotto forma di timbratura postale).

Il fatto che esso sia redatto dal responsabile non esime il titolare (o i titolari, nel caso di forme associate) da responsabilità.

E' utile suggerire, almeno per la prima stesura del Documento, che il tecnico manutentore verifichi i singoli strumenti ed attesti per ciascuno di essi la conformità e l'adeguatezza.

Il Documento deve contenere:

- l'elenco del trattamento dei dati personali

Come abbiamo sopra, rilevato è necessaria la preliminare ricognizione di tutti i trattamenti di dati personali svolti nello studio o affidati ad entità esterne.

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

E’ il c.d. mansionario della privacy, cui prima ho fatto cenno. Si tratta di individuare chi può trattare i dati personali. Appare opportuno integrare l’enunciazione della distribuzione dei compiti e delle responsabilità allegando al D.P.S. le lettere di incarico a dipendenti e collaboratori con i relativi profili di autorizzazione nonché ai terzi che possono accedere agli studi.

- analisi dei rischi che incombono sui dati.

Anche per questa voce mi richiamo a quanto precedentemente detto sottolineando come l’analisi vada principalmente indirizzata sulle circostanze possibili, probabili, prevedibili e prevenibili. Tale analisi va fatta in relazione alla natura dei dati ed agli strumenti elettronici e non.

- le misure da adottare per garantire l’integrità e la disponibilità dei dati nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità.

Questa indicazione del documento programmatico è il frutto dell’analisi dei rischi. Si devono descrivere le misure minime adottate e quelle che si intendono adottare per finalizzare ed incrementare la sicurezza, individuandole con riferimento agli strumenti elettronici, alle aree ed ai locali, alla archiviazione e custodia di atti, documenti e supporti.

Se il titolare si avvale di soggetti esterni nella predisposizione ed installazione delle misure minime di sicurezza o per la redazione del D.P.S. deve pretendere il rilascio di un certificato di conformità che garantisca la serietà dell’intervento e l’adeguatezza dello stesso alle misure di sicurezza previste.

- descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento.

Si tratta delle istruzioni scritte su chi e come deve essere gestita la fase necessaria al ripristino (in termine tecnico il Disaster recovery) dei dati persi o distrutti, a chi rivolgersi, i tempi necessari.

Il ripristino dei dati consiste nella nuova installazione dei dati persi, o danneggiati, e per far questo bisogna impartire istruzioni organizzative e tecniche per la custodia delle copie di sicurezza.

E’ specifico obbligo del titolare assicurare la possibilità di questo ripristino entro 7 giorni, affinché sia consentito il riattivo della prosecuzione delle operazioni di trattamento dei dati.

- 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 degli incaricati, a mio modesto avviso, deve essere volta alla conscenza dell’uso degli strumenti ed alla sensibilizzazione delle tematiche sulla sicurezza, facendo comprendere i rischi e le responsabilità cui vanno incontro il titolare gli incaricati (per questi ultimi anche sanzioni di natura disciplinare) che riguardano il trattamento dei dati personali.

Far conoscere i rischi connessi alla circolazione dei dati via internet, il danno che consegue, o può conseguire, alla perdita dei dati o alla loro alterazione, dare precise spiegazioni sui comportamenti da adottare nelle operazioni di trattamento, e, soprattutto, spiegare quale è la natura ed il contenuto dei dati sensibili e giudiziari su cui è necessario porre maggiore attenzione, ed in ultima analisi la regola che nel dubbio sulla natura del dato ci si rivolga al titolare. Gli incaricati hanno un ruolo fondamentale in quanto, essendo quelli più vicini al trattamento dei dati, sono quelli più esposti a diffonderli, alterarli involontariamente o provocarne la perdita ma sono anche quelli che più di altri possono con le loro indicazioni segnalare i veri rischi che incombono sui dati.

La formazione deve essere specificato nel DPS se 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.

- 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.

Vanno individuati i precisi criteri adottati ed atti a garantire che il soggetto esterno tratti i dati sensibili e giudiziari che gli sono affidati, adottando le misure minime di sicurezza prescritte dalla normativa.

Nel documento programmatico andrà indicato quali garanzie si richiedono all'affidatario, qualora tratti questi dati con strumenti elettronici, i dati che gli inviamo, anche solo in forma cartacea.

A tale riguardo segnalo ai Colleghi che per gli incarichi giudiziari (curatele, tutele, nomina di curatore o di arbitro in una vertenza che possa contenere dati sensibili o giudiziari) il Tribunale dovrebbe richiedere, quantomeno, di attestare di avere eseguito le misure minime di sicurezza.

- il successivo punto previsto per il DPS non riguarda gli studi professionali, ma concerne specifiche prescrizioni per gli organismi sanitari che trattino dati idonei a rivelare lo stato di salute e la vita sessuale, per questo non ce ne occuperemo in questa sede.

E' molto difficile immaginare un modello di documento programmatico sulla sicurezza, in quanto il suo contenuto è il frutto di un analisi e di un processo specifico per ogni singola situazione, e le fattispecie sono numerosissime.

Quello che propongo è un'ipotesi di modello che può servire da guida e che deve essere necessariamente integrato, o ripensato, dal titolare del trattamento dei dati.

avv. Antonio F. Rosa

Verona, via Rosa 8

Tel. 0458002239

Email rosa-ferrarese@iol.it

Bibliografia: Segnalo per la semplicità e chiarezza nell'esposizione, anche dei dati tecnici, i lavori "Il manuale della privacy" ed "Il nuovo codice privacy: che fare?" di M. Bernasconi e Lorenzo Riva della Diamint.com Srl (scaricabili via internet) ed ai quali ho fatto riferimento per le note di cui sopra. ; "Guida pratica alle nuove misure di sicurezza per la privacy" F. Berghella , e il Riem "Privacy e sicurezza", Edizione Simone.

Modello di Documento programmatico sulla sicurezza nel trattamento dei dati personali

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato dallo Studio Legale ……..

Il presente documento è stato redatto da……..in qualità di titolare/ responsabile per la sicurezza, che provvede a firmarlo in calce

Elenco dei trattamenti di dati personali

Lo Studio Legale tratta i seguenti dati:

dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;

dati comuni del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;

dati comuni dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;

dati comuni di terzi, forniti dai clienti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari;

dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;

dati comuni di altri Avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;

dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente, o l'adesione ad organizzazioni sindacali;

dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;

dati sensibili dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;

dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;

dati sensibili di clienti o terzi, comunque afferenti la vita sessuale.

I dati non pubblici vengono acquisiti previa l'informativa che si allega al presente D.P.S.

Questi dati vengono trattati e conservati in fascicoli riposti in schedari dotati di chiusura, nonché trattati tramite computer in rete in locali protetti e con accesso ad internet, archiviati al termine della pratica.

Lo studio, ove vengono trattati i dati, è ubicato in un condominio in zona centrale, dotato di portone di ingresso a chiusura automatica e con videocitofono, con sorveglianza notturna, e porte blindate. Sito al primo piano. I singoli studi, che lo compongono, sono dotati ciascuno di porta con chiusura a chiave, così come l'archivio.

La segreteria è ubicata in un locale più ampio, dove in una zona separata e ben distanziata dalle postazioni di lavoro delle segretarie, è ricavata una sala di attesa per i clienti.

Lo studio è dotato di cassaforte con chiusura a chiave.

Ogni studio è dotato di un computer in rete e connesso ad internet con connessione ADSL in rete, eccezione fatta per la sala biblioteca dove sono ubicati due computer in rete e con connessione ADSL ad internet; nel più ampio locale, ove è ubicata la segreteria si trovano due postazioni di lavoro con computer con connessione ADSL ad internet ed in fianco ad una di esse è ubicato il server connesso ad internet ed il router per la connessione ad internet. Inoltre in questo locale si trovano le stampanti, il fax, la fotocopiatrice e lo scanner. Uno dei due computer è dotato di separato modem per l'utilizzo di Winfax. Le linee telefoniche sono due ISDN.

Il sistema operativo del server è ……..

Il sistema operativo dei computer è……..

Lo studio adopera Internet Explorer versione …..

Lo studio adopera OutlooK Express ……..

Lo studio per adopera per a gestione il sistema……

Antivirus adoperato ……..

Firewall adoperato …….

Titolare del trattamento è l'avv……..

Responsabile del trattamento è ……..

Amministratore del sistema è ……..

Incaricati del trattamento sono:

Dr. …….. (collaboratore di studio)

Dr. …….. (collaboratore di studio)

…….. (dipendente)

…….. (dipendente)

Tecnico incaricato dell'assistenza e manutenzione degli strumenti elettronici è ……..

I dati comuni dei clienti, dei fornitori o di terzi, i dati comuni di altri Avvocati e professionisti cui lo studio affida incarichi o si rivolge per consulenze, i dati giudiziari dei clienti, i dati giudiziari di terzi, i dati sensibili dei clienti e di terzi sono trattati, oltre che dal titolare, anche da tutti gli incaricati.

I dati comuni del personale dipendente, i dati sensibili del personale dipendente, i dati afferenti i pagamenti a favore di terzi fornitori, la contabilità e i rapporti bancari dello studio sono esclusivamente tenuti dalla dipendente……., che si occupa della amministrazione. Questi dati non sono in rete ma si trovano solo sul computer della segretaria autorizzata a trattarli.

E' stata compiuta l'analisi dei rischi che si può così sintetizzare:

per i dati comuni del personale dipendente (quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi, ai rapporti fiscali), i dati comuni dei clienti (dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, compresi i dati sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi), i dati comuni di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio, compresi i dati

sul patrimonio e sulla situazione economica, o necessari per disposizioni fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari) i dati comuni dei fornitori (concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) i dati comuni di altri avvocati e professionisti cui lo studio affida incarichi (quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai rapporti fiscali) ed i dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali: il rischio legato alla loro gestione può definirsi basso/medio

Per i dati sensibili del personale dipendente, i dati giudiziari dei clienti,i dati giudiziari di terzi, i dati sensibili dei clienti (dagli stessi forniti per l'espletamento degli incarichi affidati allo studio) i dati sensibili di terzi (forniti dai clienti per l'espletamento degli incarichi affidati allo studio) il rischio legato alla loro gestione è da definirsi medio, eccezion fatta per i dati riguardanti le pratiche in cui sono contenuti dati idonei a rivelare lo stato di salute, o dati giudiziari di clienti o terzi e le pratiche, quali quelle in materia di diritto familiare, con dati idonei a rivelare la vita sessuale. Per questi ultimi dati il rischio collegato alla gestione può definirsi alto. Per i dati sensibili afferenti cause di stato (esempio disconoscimento di paternità) il rischio di gestione può essere definito maggiormente elevato.

Gli strumenti elettronici sono:

nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da ……. marca …….. modello ……

nr. 1 computer connesso in rete ed a internet nella segreteria utilizzato da ……. marca …….. modello …..

nr. 1 computer server connesso in rete ed a internet nella segreteria marca ……. modello ……

nr. 1 computer connesso in rete ed a internet nello studio dell'avv. ……. utilizzato dallo stesso marca ….. modello ……..

nr. 1 computer connesso in rete ed a internet nello studio dell'avv. ……. utilizzato dallo stesso marca …… modello ……..

nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da ……. marca ……. modello ……..

nr. 1 computer connesso in rete ed a internet nella biblioteca utilizzato da …….. marca ……. modello ……..

Per quanto riguarda gli strumenti elettronici, possono verificarsi malfunzionamenti, guasti, eventi naturali, alterazioni delle trasmissioni.

Per quanto riguarda i software contenuti negli strumenti elettronici, possono verificarsi errori, virus, intercettazioni dei dati.

Per quanto riguarda le aree ed i locali: possono essere colpiti da eventi naturali o accessi di terzi non autorizzati.

Per ridurre i rischi sono state adottate le seguenti misure:

Autenticazione informatica, tale misura è stata adottata dotando ciascun incaricato di una password di almeno 8 caratteri (o minore per le caratteristiche del sistema). Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore, né allo studio legale. La stessa viene autonomamente scelta dall'incaricato e dallo stesso custodita in una busta chiusa che viene consegnata al titolare del trattamento, il quale provvede a metterla nella cassaforte dello studio in un plico sigillato. Ogni tre mesi ciascun incaricato provvede a sostituire la propria password. Si è altresì disposto che le password vengano automaticamente disattivate dopo tre mesi di non utilizzo.

Inoltre si è disposto che a tutti gli utilizzatori di strumenti elettronici non lascino incustodito, o accessibile, lo strumento elettronico stesso.

A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo screensaver automatico dopo 1 minuto di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.

Si è inoltre disposto che essi verifichino la provenienza delle email e non operino operazioni di sharing.

Essendo gli incaricati autorizzati a trattare la quasi totalità dei dati, e comunque quelli sensibili e giudiziari, non si è provveduto a dare disposizioni in caso di prolungata assenza o impedimento dell'incaricato, eccezion fatta per i dati trattati in via esclusiva dal dipendente ……., che cura la contabilità, per il quale è stato indicato per iscritto il nominativo dell'incaricato della sostituzione.

Ogni singolo computer è dotato di dispositivo antivirus di marca ……., che viene aggiornato con funzione automatica e con scansione per ogni aggiornamento antivirus, e comunque settimanale.

Sul server è stato installato firewall di marca …….

Per ogni singolo computer è prevista la funzione di aggiornamento automatico del sistema fornito dalla Microsoft mediante lo strumento windows – update.

Analogo sistema di aggiornamento automatico è previsto per l'antivirus. E' stata data istruzione che, qualora nessun aggiornamento del sistema fosse segnalato automaticamente per un periodo di mesi 6, si provveda comunque ad attivare la funzione di controllo per verificare l'esistenza o meno di detti aggiornamenti automatici.

E' stato disposto l'obbligo di provvedere ad un backup settimanale dei dati e dei sistemi installati sul server su cd rom, i quali vengono conservati e chiusi in un cassetto, e si è data disposizione di verificare, effettuato il backup, la leggibilità del supporto e che una volta a settimana si proceda a verifica a campione della leggibilità dei dati; custode di detti backup è stato nominato l'incaricato ……. Si è data disposizione che, effettuato un backup, venga distrutto il c.d. precedente.

Si è data disposizione che, terminata la trattazione di una pratica, ogni relativo file, o dato, esistente sui computer, sia cancellato.

Si è disposto che non siano lasciati incustoditi sulle scrivanie, o su altri ripiani, atti, documenti e fascicoli delle pratiche. I fascicoli vanno conservati negli appositi schedari e prelevati per il tempo necessario al trattamento per esservi poi riposti.

Le comunicazioni a mezzo posta, o a mezzo telefax, dovranno essere tempestivamente smistate e consegnate ai destinatari. Quando è dato un ordine di stampa, il documento stampato dovrà essere prontamente prelevato e consegnato all'interessato.

Il locale destinato all'archivio dovrà essere chiuso a chiave. La dipendente …….. è incaricata di controllare l'accesso all'archivio. Fuori dall'orario di lavoro l'accesso all'archivio è consentito previa registrazione.

Si è data istruzione che il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti sia riposto negli appositi sacchi di plastica e che detti sacchi siano chiusi in modo che atti e documenti negli stessi contenuti non possano accidentalmente fuoriuscire, e che detto materiale sia giornalmente asportato.

Il rischio di accesso ai locali dello studio, può essere definito basso, atteso che l'ingresso allo studio è controllato, e che lo studio è dotato di videocitofono e chiusura con porta blindata.

Il rischio di accesso ai singoli studi può essere definito basso, atteso che gli stessi sono dotati di porte con chiusura e l'ingresso di terzi estranei avviene solo previa accettazione e controllo.

Il rischio di accesso ai singoli strumenti da parte di persone non autorizzate può essere definito basso, essendo controllato l'accesso allo studio da parte di terzi; la zona di attesa dei clienti distanziata dagli strumenti ed essendo gli stessi clienti controllabili dalla segreteria.

Le aree ed i locali potrebbero essere interessati da eventi naturali, quali incendi, allagamenti e corto circuiti, pur avendo lo studio provveduto ad adottare le disposizioni di sicurezza stabilite dalla L. 626/94. Essendo lo studio dotato di dispositivi salvavita, il rischio può comunque definirsi basso.

Per quanto riguarda gli strumenti elettronici, il rischio può essere definito basso, essendo state adottate dallo studio le misure di sicurezza, tendenti a ridurre il rischio gravante sui dati e derivante dalla gestione di detti strumenti.

Per quanto riguarda la documentazione cartacea, il rischio può essere definito basso, essendo l'archivio chiuso a chiave, gli schedari chiusi, ed essendo state adottate le altre misure indicate, fatta eccezione ovviamente per gli eventi naturali.

I telefax inviati su carta chimica sono stati riprodotti su carta normale per evitarne il deterioramento.

Per quanto riguarda i supporti di memorizzazione, il rischio di deterioramento dei dati da essi portati può essere ritenuto basso, attesi i frequenti back up, ed il fatto che essi sono conservati in un cassetto chiuso a chiave, così come i dischi di installazione dei programmi software adottati.

Non vi sono elaboratori non in rete, non vi sono elaboratori non in rete e connessi ad internet, per cui nessun giudizio di rischio deve essere dato su detti strumenti.

Atteso –infine- che gli incaricati al trattamento dei dati sono qualificati ed affidabili e dimostrano riservatezza ed attenzione nella gestione dei dati stessi, il rischio afferente la riservatezza, o la distrazione, o l'incuria degli stessi, può essere definito basso.

Inoltre i dati, quanto comuni che sensibili, per gli affari trattati dallo Studio ed il tipo di clientela dello Studio non paiono essere, come detto, di particolare interesse per terzi.

Si ritiene che verranno adottate le seguenti ulteriori misure.

Entro il termine del 30.06.2004 sarà installato sistema di firma elettronica per la trasmissione delle e-mail.

Sarà inoltre adottata ogni altra misura che dal tecnico della manutenzione venisse ritenuta utile e necessaria per migliorare la sicurezza degli strumenti elettronici.

Sarà installato inoltre gruppo di continuità per il server.

Nell'ipotesi di distruzione o danneggiamento dei dati o degli strumenti elettronici, si predisporrà entro il 30.06.2004 apposito piano di ripristino degli stessi, impartendosi comunque sin d'ora le seguenti istruzioni:

- avvertire il titolare del trattamento dei dati e l'incaricato che ha in custodia il c.d. di back up nonché i c.d. contenenti i vari software dello studio installati sugli strumenti elettronici;
- rivolgersi immediatamente e chiedere l'intervento del tecnico manutentore della ditta ..... sollecitandone al più presto l'assistenza;
- reinstallati i programmi danneggiati o distrutti, sempre che non sia necessario sostituire l'intero hardware, provvedere a reinstallare tutti i dati contenuti nel c.d. di back up;
- provvedere all'aggiornamento dei sistemi operativi una volta reinstallati;
- verrà dato incarico al tecnico manutentore di suggerire ogni altra misura;
- in ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni;
- al fine di evitare eventi di perdita e di danneggiamento degli strumenti elettronici e dei datti in essi contenuti, si prevede che per due volte all'anno sia effettuata manutenzione in modo adeguato dal tecnico incaricato.

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Essa tende a sensibilizzare gli incaricati sulle tematiche di sicurezza, facendo comprendere i rischi e le responsabilità (con specificazione delle sanzioni connesse penali e disciplinari) che riguardano il trattamento dei dati personali.

Inoltre, essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e giudiziari, con l'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare se un dato possa avere o meno natura sensibile o giudiziaria.

La formazione è fatta dal titolare dello studio.

Nel caso in cui il trattamento dei dati sensibili e/o giudiziari venga affidato a soggetti esterni, che li trattino con strumenti elettronici, per avere la garanzia che essi adottano le misure minime di sicurezza si esigerà dagli stessi una dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale attestino di aver adottato le misure minime previste dal disciplinare.

Alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio, viene dato incarico scritto con richiesta di specificazione dei nomativi delle persone che accedono ed espresso invito a limitarsi alle sole attività pertinenti alla prestazione per cui accedono.

Si allegano oltre l'informativa, la lettera di istruzioni agli incaricati, la lettera alle ditte che provvedano ad effettuare prestazioni che comportano accesso di estranei allo studio.

Verona, lì

Il titolare

Modello predisposto da: Avv. Antonio F. Rosa

Foro di Verona

Bibliografia: "Il nuovo codice privacy: che fare?" di M. Bernasconi e Lorenzo Riva della Diamint.com Srl

Gruppo di Iniziativa Forense

Con il patrocinio dell'Ordine degli Avvocati di Verona
Con il patrocinio del Consiglio e Collegio Notarile di Verona

Incontro sul tema

Privacy e studi legali
Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico

Verona 27 febbraio 2004 ore 15,30

PROPOSTA DI DOCUMENTO PER L'INFORMATIVA E CONSENSO NEGLI STUDI LEGALI

Avv. Andrea Turco – foro di Verona

Necessaria premessa a questo mio intervento deve essere la precisazione che il documento così come mi accingo a presentarvi non vuol essere certo unica ed assoluta soluzione interpretativa ad una disposizione di legge (il D.Lgs.n.196/03) di fronte alla cui complessità ed impianto articolato ho semplicemente ritenuto di adottare – anche con il conforto dei Colleghi relatori con cui non è certo mancato il confronto critico – una soluzione che, ovviamente nel pieno rispetto di quanto prescritto, garantisse e tutelasse il più possibile tanto il professionista quanto il Cliente.

Ed è proprio per tale ragione che, anche raccogliendo I consiglio della Collega Avv. Bonanno, il documento in oggetto è stato costruito, "*adottando le garanzie più complete, con il massimo formalismo richiesto riportando le norme di legge non tanto in modo anonimo ed aspecifico quanto piuttosto in maniera determinata e proporzionata – in senso spaziale e temporale – agli usi professionali*".

Ed è ancora per le stesse ragioni appena riferite che ho ritenuto conveniente predisporre il documento *de quo* in modo che l'autorizzazione in esso contenuta potesse abbracciare il trattamento di qualsiasi tipo di dato senza, dunque, essere costretti a distinguere tra trattamento

stragiudiziale che necessiterebbe dell'autorizzazione da parte dell'interessato e trattamento giudiziale che – al contrario – esonererebbe il professionista dal richiedere ed ottenere la preventiva autorizzazione.

Non va, infatti, dimenticato, come già illustrato dalla Collega Bonanno, che l'Avvocato – secondo quanto contenuto nelle autorizzazioni n.4 e 7 così come emanate dal Garante della Privacy – è stato esonerato, per il trattamento in sede giudiziale dei dati sensibili, dal dover preventivamente richiedere autorizzazione a quel medesimo utilizzo. Inoltre, non va parimenti sottovalutato quanto espressamente indicato e già ricordato al punto "b" dell'art.24 del D.Lgs.n.196/03 ove si legge che il consenso non è richiesto per adempiere ad un obbligo derivante da un contratto di cui è parte l'interessato (come appunto può dirsi il MANDATO ALLE LITI).

Orbene, ricordata brevemente ma a ragione la complessità della norma da cui si è partiti per approdare a quanto mi accingo a proporvi, vado – quindi – ad illustrarvi la struttura ed il contenuto della **"Dichiarazione di autorizzazione al trattamento dei dati personali – identificativi – sensibili e giudiziari ex D.Lgs.n.196/03".**

LA STRUTTURA: Il documento è articolato in 9 punti e 7 sottopunti (tutti concentrati nella spiegazione del punto n.3) oltre che in n.7 note poste ad ulteriore specificazione e chiarimento di quanto mano mano illustrato nei vari passaggi dell'autorizzazione.

IL CONTENUTO:

- ***facciata di presentazione:***

va innanzitutto sottolineato come al fine di conferire maggior incisività a quanto inserito nel documento in esame, la dichiarazione di autorizzazione al trattamento è stata predisposta come se provenisse direttamente dall'Interessato e, quindi, in prima persona. Tant'è che la prima facciata del documento è interamente dedicata alla raccolta dei dati identificativi dell'interessato che, nella sua definizione concettuale così come fornita dall'art.4 comma 1 lettera "i" riportata, potrà essere tanto persona fisica quanto persona giuridica piuttosto che ente e/o associazione. E come sopra ricordato gli interessati forniranno i loro dati nella forma diretta più normale e cioè secondo lo schema di "Io sottoscritto …" ovvero "La Ditta o la Società … " a cui faranno seguito gli ulteriori elementi identificativi che

dovranno necessariamente accompagnare il nome ed il cognome o la denominazione sociale.

- ***Punti 1 e 2:***

al punto "1" del documento si fa espresso richiamo all'art.23 del D.Lgs.n.196/03 racchiuso nella PARTE I (Disposizioni Generali), TITOLO III (regole Generali per il Trattamento dei dati), CAPO III (Regole ulteriori per privati ed enti pubblici economici). In particolare l'art.23 è titolato "Consenso" e, come è facile intuire anche dalla sua collocazione, è norma **generale** e, quindi, valida anche per la categoria di soggetti c.d. privati tra cui possono sicuramente essere inseriti anche gli Avvocati che nella loro qualità di *difensori* possono certamente qualificarsi "privati" ai sensi della legge sulla privacy, anche se in concreto e per altro verso la loro attività risponde ad esigenze di pubblica necessità.

Ecco, perchè, nell'ambito più generale del dovere di informativa così come imposto si è ritenuto di rendere edotto l'interessato – o meglio, vista l'impronta data al documento, di far dichiarare all'interessato in prima persona che è a conoscenza – del fatto che il trattamento dei dati personali da parte di privati è ammesso solo con il suo consenso espresso che deve essere **fornito liberamente** e con **specifico riferimento ad un trattamento individuato** oltre che **documentato per iscritto e preceduto dall'informativa di cui all'art.13 D.Lgs.n.196/03**.

Non a caso, poi, si è distinto quanto appena riferito da quanto proposto al successivo "**PUNTO 2**" dal momento che in quest'ultimo caso si è ripreso quanto ulteriormente esplicitato dallo stesso art.23 ma al suo comma IV ove si fa riferimento al trattamento dei dati c.d. sensibili. In particolare l'art.23 si esprime con terminologia differente rispetto a quanto prescritto in tema di trattamento di dati personali. Infatti, se in quest'ultimo caso il **consenso deve essere documentato per iscritto**, per ciò che riguarda il trattamento dei dati sensibili, invece, è previsto che il **consenso sia manifestato in forma scritta**.

Ora, non è ben chiaro che cosa il Garante abbia voluto dire attraverso l'utilizzo di espressioni del genere appena ricordato, ma è chiaro che al fine di non pregiudicare la posizione di chi quei medesimi dati (con ciò riferendoci a qualsiasi tipo di dato) andrà a trattare si è ritenuto conveniente soffermarsi sul fatto che in entrambe le ipotesi si parla di **consenso**

comunque scritto e che, pertanto, se manifestato piuttosto che documentato sarà utile acquisirlo attraverso una autorizzazione comunque da doversi far sottoscrivere dall'interessato.

Nel medesimo '**PUNTO *2***' è stata, poi, esplicitata una deroga a quanto detto in tema di trattamento dei dati sensibili. In particolare è stato inserito un richiamo a quanto previsto dall'**art.26 comma 4 lettera "c"** che chiarisce come **i dati sensibili possano essere oggetto di trattamento anche senza il consenso** quando il trattamento sia necessario per lo svolgimento delle investigazioni difensive di cui alla L.397/2000 o quando servano per far valere in giudizio un diritto sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Sempre al fine di fornire una "informativa" il più possibile chiara e trasparente, la norma di cui alla deroga appena ricordata è dettagliatamente ed integralmente riportata alla **nota n.1** posta in calce al documento.

Con particolare riferimento alle **note**, compresa quella appena indicata, va chiarito che ogni volta che si è ritenuto di inserirne una si è anche previsto che del loro contenuto l'interessato dichiarasse non soltanto di essere stato informato ma anche che quanto oggetto di preventiva illustrazione corrispondesse – comunque – al contenuto delle note stesse.

E ciò ci è utile, anche, per passare all'analisi del successivo punto 3.

- ***Punto 3:***

è, questo, punto fondamentale oltre che di tutto il documento (tanto che si articola in n.7 sottoppunti ed il suo testo integrale viene riportato alla **nota 2** posta in calce alla stessa autorizzazione) anche dello medesimo D.Lgs.n.196/03. La norma in commento disciplina il **dovere di informativa** da parte del titolare nei confronti dell'interessato; titolare che – come recita espressamente la norma – potrà informare l'interessato sia oralmente che per iscritto, ma – comunque ed è ciò che più conta – sempre **preventivamente al trattamento stesso**.

Orbene, l'art.13 racchiude e prescrive una serie di informazioni da rendere all'interessato che – nel documento predisposto – vengono tutte specificatamente indicate e riportate ai punti da "a" a "g" compresi, e cioè:

a) FINALITA' e MODALITA' DI TRATTAMENTO:

che, per quel che qui ci interessa, vanno rispettivamente identificate come segue:

- per quel che riguarda le **finalità**: il trattamento avverrà in ambito legale / giudiziario in conformità allo scopo per cui è stato conferito mandato o per finalità – comunque – connesse e/o strumentali allo svolgimento degli incarichi affidati;
- per quel che riguarda le **modalità**: nel rispetto della normativa vigente e fermi gli obblighi di riservatezza e segreto professionale.

b) FACOLTATIVITA' DEL CONFERIMENTO DEI DATI:

nel senso che l'interessato deve essere informato che può anche rifiutarsi di fornire i dati che gli vengono richiesti e, quindi, non deve a ciò sentirsi obbligato. Tale informazione, però, deve essere accompagnata da quella ulteriore che informa l'interessato, e veniamo al successivo punto "c", su

c) CONSEGUENZE DI UN EVENTUALE RIFIUTO:

cioè, l'interessato deve essere messo a conoscenza del fatto che, pur essendo una sua facoltà – laddove decidesse o ritenesse di non assecondare il richiesto **conferimento di dati** – il mandato ed in genere gli incarichi professionali richiesti, oltre che la prosecuzione di quelli in corso, potranno non essere accettati e/o proseguiti e, dunque, espletati.

d) SOGGETTI o CATEGORIE DI SOGGETTI AI QUALI I DATI PERSONALI POSSONO ESSERE COMUNICATI o CHE POSSONO VENIRNE A CONOSCENZA IN QUALITA' DI RESPONSABILI O INCARICATI e L'AMBITO DI DIFFUSIONE DEI DATI MEDESIMI:

al fine di meglio chiarire la portata del presente punto distinguiamo tra:

- ambito e soggetti esterni a quello del titolare: indicati genericamente in tutti i soggetti Privati e/o Pubblici, oltre che nelle competenti Autorità Giudiziarie nonché nei soggetti in quelle tesse sedi preposti al loro recepimento e/o trattamento;
- ambito interno allo stesso titolare: indicati negli Avvocato/i titolare/i dello studio , nell'eventuale responsabile o incaricati designati (relativamente ai quali le rispettive funzioni sono state specificate all'interessato e, quindi, riportate alla **nota n.4** posta in calce al documento), oltre che nei

collaboratori di studio, nei praticanti e nelle segretarie (le quali ultime, in particolare, potranno venire a conoscenza dei dati dei Clienti, per la redazione della nota spesa).

N.B. – un nota bene va fatto per ciò che concerne l'ulteriore specificazione contenuta nel punto "d" in commento e cioè a quella che rimanda al **DPS** per la specifica indicazione tanto delle MISURE DI SICUREZZA adottate quanto, per gli aggiornamenti e/o le eventuali modifiche, dei TITOLARI, dei RESPONSABILI e/o degli INCARICATI (con l'ulteriore precisazione che, con riferimento particolare a questi soggetti, i dati iniziali vengono comunque già forniti ai successivi punti "f" e "g").

e) DIRITTI DELL'INTERESSATO EX ART.7 D.LGS.N.196/03:

punto di particolare importanza dal momento che informa l'interessato sui suoi diritti in ordine al trattamento dei suoi dati. Il testo integrale dell'art.7 – titolato "Diritto di accesso ai dati personali ed altri diritti" – è stato riportato alla **nota n.5** posta in calce al documento e sostanzialmente può essere così schematizzato:

- diritti di cui al comma 1: l'interessato ha **diritto di avere conferma** sull'esistenza o meno di suoi dati presso un determinato soggetto e, conseguentemente, di averne comunicazione in forma intelligibile;
- diritti di cui al comma 2: l'interessato ha **diritto ad ottenere** informazioni sull'origine dei dati personali, sulle finalità e modalità di trattamento, sulla logica applicata in caso di trattamento con l'ausilio di strumenti elettronici, sugli estremi identificativi dei titolari, eventuali responsabili e/o incaricati, sui soggetti ai quali i dati possono essere comunicati in qualità di responsabili e/o incaricati;
- diritti di cui al comma 3: l'interessato ha **diritto di ottenere** l'aggiornamento, rettificazione, integrazione, cancellazione, trasformazione in forma anonima o 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 trattati con conferma che tali operazioni sono state portate a conoscenza anche di tutti quei soggetti a cui i dati sono stati comunicati e/o diffusi, salvo che ciò non sia impossibile o attuabile soltanto con mezzi manifestamente sproporzionati rispetto al diritto tutelato.
- diritti di cui al comma 4: l'interessato ha **diritto di opposizione totale o parziale** per motivi legittimi al trattamento dei dati personali che lo riguardano sia che siano pertinenti allo scopo per cui sono stati raccolti sia che siano stati utilizzati per l'invio di materiale pubblicitario o il compimento di ricerche di mercato o comunicazioni commerciali.

f) <u>ESTREMI IDENTIFICATIVI DEI TITOLARI DEL TRATTAMENTO</u>:

con tale punto – salvo eventuali e successive modifiche e/o aggiornamenti per cui si è già prima fatto presente il rimando al DPS – all'interessato vengono forniti gli estremi identificativi del o dei titolari del trattamento che nel nostro caso corrisponderanno con i titolari dello studio o dell'associazione.

g) <u>ESTREMI IDENTIFICATIVI DEL RESPONSABILE E DEGLI INCARICATI DEL TRATTAMENTO</u>:

anche in tal caso l'interessato viene reso edotto degli estremi identificativi dell'eventuale responsabile del trattamento con la precisazione che ogni sua modifica verrà prontamente comunicata.
Per quanto concerne, invece, i dettagli relativi alle ditte di assistenza software e hardware dei sistemi dello studio nonché dello studio commercialista, a cui i dati verranno comunicati al solo fine di poter fa fronte ai normali adempimenti fiscali, il documento rimanda a quanto meglio descritto nel DPS.

- ***<u>Punto 4</u>:***

nel punto in commento vengono fornite due ulteriori precisazioni:

- <u>in primo luogo</u>: l'interessato viene reso edotto del fatto che i dati verranno trattati – nell'espletamento del mandato e/o incarico ricevuti – nei limiti di cui alll'**art.25 D.Lgs.n.196/03 titolato "Divieti di Comunicazione e Diffusione"** (il cui testo integrale viene riportato alla **nota 6** posta in calce al documento) e cioè: senza che gli stessi dati possano essere comunicati e/o diffusi qualora ne sia stata ordinata la cancellazione ovvero sia decorso il termine di tempo indicato all'art.11 lettera "e" ove è stabilito che i dati vengano conservati per il tempo strettamente necessario e quindi non superiore a quello necessario per gli scopi per cui sono stati raccolti e successivamente trattati;

- <u>con riferimento a quest'ultimo richiamo – quello del periodo così come indicato all'art.11 lettera "e" – si rimanda, però, a quanto si dirà al successivo PUNTO 6.</u>

- <u>in secondo luogo</u>: l'interessato viene reso edotto del fatto che, nell'espletamento dell'incarico ricevuto e nel perseguimento delle finalità

già meglio esplicitata al punto “a”, i dati potranno essere oggetto oltre che di trattamento anche di **comunicazione** oltre che di **diffusione** nell’accezione dei relativi termini così come rispettivamente indicata dall’art.4 comma 1 lettere “a, l ed m”; definizioni che – anche in tale caso – vengono integralmente riportate alla **nota 7** posta in calce al documento.

- ***Punto 5:***

sempre nell’ottica di massima trasparenza che pervade l’intera struttura e contenuto della presente autorizzazione, l’interessato viene reso edotto e, perché no, rassicurato sul fatto che il trattamento dei suoi dati avverrà garantendone la sicurezza e riservatezza attraverso – anche e non soltanto – l’ausilio di strumenti elettronici che ne consentano la memorizzazione, gestione e trasmissione.

- ***Punto 6:***

riprendendo quanto già anticipato commentando il punto 4 che precede, nel presente punto 6 viene dato atto che l’interessato è consapevole che i suoi dati verranno conservati oltre l’esecuzione degli incarichi affidati e precisamente per il periodo di 10 anni.

N.B. – Orbene, con riferimento a quanto appena illustrato va tenuto presente quanto segue. Come già anticipato dall’Avv. Bonanno, in relazione alla **conservazione dei dati personali** (ed in particolare per quelli **giudiziari**) si pone il problema della durata del diritto del professionista alla loro conservazione dopo l’esaurimento dell’incarico. Infatti:

- non soltanto: l’art.11 lettera “e” prescrive la cancellazione dei dati nel momento in cui il loro mantenimento “*in vita*” dovesse essere incompatibile con il conseguimento del risultato per cui è stato rilasciato mandato o conferito incarico;
- ma anche: l’art.27 prescrive che il trattamento – e quindi anche la conservazione che di quel concetto più generale rappresenta un’estrinsecazione – dei dati giudiziari da parte di privati è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

Il fatto è, però, che se ciò è vero non va – comunque – dimenticato che si deve, però, fare i conti con una serie di norme e cioè:

- quella per cui il professionista, **da un punto prettamente fiscale**, è tenuto a conservare la documentazione per almeno 5 anni dalla chiusura della pratica a cui inerisce;
- quella che deriva direttamente dal rapporto di mandato tra il professionista (mandatario) ed il Cliente (mandante) in virtù della quale il diritto di quest'ultimo a ottenere quanto consegnato al primo si prescrive nel termine di 10 anni. Il tutto, poi, senza dimenticare che a prescindere da ciò si è sempre e comunque ritenuto, probabilmente proprio per tale ragione, di dover custodire i fascicoli di studio per almeno 10 anni;
- quella di cui all'art.2961 cod.civ. che in tema di prescrizioni presuntive stabilisce che gli Avvocati, sono esonerati dal rendere conto degli incartamenti (che secondo una interpretazione più estensiva del concetto, comprenderebbero non soltanto quelli relativi ad affari contenziosi ma anche documenti riguardanti la preparazione di pareri, schemi contrattuale, etc.) relativi alle liti dopo 3 anni da che queste sono state decise o altrimenti terminate.

Alla luce di quanto appena premesso, quindi, nasce un'imprescindibile **NECESSITÀ DI COORDINARE I PRECETTI NORMATIVI INDICATI.**

Pertanto:

- atteso il diritto dell'interessato a poter richiedere quanto consegnato al professionista entro il termine di prescrizione ordinaria di 10 anni così come stabilito dall'art.2946 cod.civ. (il che è un suo innegabile diritto derivante da un rapporto di mandato perfezionatosi con il professionista);
- atteso il fatto che normalmente il professionista per questioni meramente fiscali è tenuto dalla legge a conservare documentazione giustificante la propria attività per un periodo non inferiore ai 5 anni;
- atteso che l'art.2961 cod.civ. non può comunque trovare applicazione concreta per quel che ci riguarda stabilendo un termine di prescrizione **presuntiva** di tre anni tanto a favore del Cliente (nei confronti del quale qualora il professionista gli chiedesse il pagamento oltre i tre anni potrebbe opporre l'intervenuta prescrizione presuntiva del suo diritto ad ottenerlo) quanto nei confronti dello stesso professionista (che potrebbe sempre deferire al cliente il giuramento decisorio per provare

l'intervenuta consegna dell'incartamento che lo riguarda e/o il suo diritto ad essere pagato);

ALLA LUCE DI TUTTO QUANTO PRECEDE:
non necessitando di autorizzazione alcuna la custodia per il termine di 5 anni nascendo da un obbligo di legge che il D.Lgs.n.196/03 non sembra derogare ed essendo, comunque, un diritto garantito ex lege a tutela dell'interessato quello tutelato dall'art.2946 cod.civ., si è comunque ritenuto di inserire la precisazione di cui al punto 6 in commento al solo ed unico scopo di rendere ancor più trasparente il contenuto del documento autorizzativo.

- ***Punto 7:***

venendo al punto 7, si precisa che il suo contenuto non va visto come contraddittorio rispetto a quello del punto 6 che precede. Infatti se il precedente punto riguardava la custodia del cartaceo, quello in esame riguarda il trattamento dei dati con l'ausilio di strumenti elettronici.
In questo caso, l'interessato è reso edotto del fatto che all'esaurimento dell'incarico conferito si procederà alla **cancellazione** di quei dati che non risultino pertinenti ed eccedenti eventuali ed ulteriori incarichi che dovessero essere conferiti dal medesimo Cliente.

- ***Punto 8:***

ancora una volta e sempre al fine di garantire la massima trasparenza ed informativa dell'interessato, nel punto in commento si fa espresso riferimento all'**art.52 del D.Lgs.n.196/03** che consente all'interessato – che abbia motivi legittimi per farlo – di chiedere con domanda da depositarsi nella cancelleria dell'autorità competente prima che sia definito il relativo grado di giudizio, che sull'originale della sentenza o dell'emanando altro provvedimento sia apposta un'annotazione volta a precludere – in caso di riproduzione della sentenza o del provvedimento in qualsiasi forma per finalità di informazione giuridiche su riviste di settore, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o sul provvedimento.

- ***Punto 9:***

infine, dal momento che più che verosimilmente potrà capitare che il medesimo cliente sia tutelato dallo stesso professionista in più vertenze si è voluto conferire **efficacia retroattiva** alla presente autorizzazione rendendola valida anche per le posizioni aperte prima dell'entrata in vigore del nuovo Codice sulla Privacy (D.Lgs.n.196/03). Per fare ciò, alla semplice espressione "*l'informativa dovrà ritenersi valida anche per le posizioni aperte prima del 01.01.2004*" si è ritenuto di accompagnare l'elenco specifico delle pratiche a cui l'autorizzazione deve estendere la propria portata.

UN ULTIMO APPUNTO:

nella parte finale dell'autorizzazione e precisamente nella parte ove vi è la formale dichiarazione di autorizzazione è stata esplicitato che "*per l'eventuale fase giudiziale verrà rilasciato apposito mandato nelle forme di legge*".
Ciò è stato fatto la fine di evitare – per quanto possibile – fraintendimento sul fatto che **l'informativa sia stata resa precedentemente al trattamento dei dati e, quindi, all'esecuzione dell'incarico o all'espletamento del mandato.**
Ci si rende conto che un documento del genere in esame **non ha sicuramente data certa fino a che non gliela si conferisca nei modi di legge**. Il che sarebbe, peraltro, assurdo.
In ogni caso si spera in tal modo di evitare problemi che in tal senso potrebbero porsi.

N.B. Si precisa che nella presente relazione e nel relativo documento non è stato affrontato il problema degli studi legali che – avendo contatti con l'estero (paesi appartenenti alla UE piuttosto che terzi) – possono essere soggetti a trasferimento transfrontaliero di dati. In particolare ci si vuol riferire agli artt. da 42 a 45 D.Lgsn.196/03 compresi.

§§§

Qui di seguito, quindi, sono ad allegarVi il documento oggetto della mia proposta e commento nell'intervento che precede:

DICHIARAZIONE DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI, IDENTIFICATIVI, SENSIBILI e GIUDIZIARI ex D.LGS. 30 giugno 2003 n.196

PERSONA FISICA

Io sottoscritto/a _____

nato/a il _____ a _____

residente a _____

in Via _____

cod.fisc. _____

qui di seguito identificato/a, anche, con il termine "*interessato/a*" nel significato di cui alla lettera "i" dell'art.4 D.Lgs.n.196/03 e cioè di: "*persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali*".

PERSONA GIURIDICA

la Ditta / Società _____

con sede a _____

in Via _____

cod.fisc. / partita I.V.A. _____

in persona di _____

nella sua qualità di _____

nato/a il _____ a _____

residente a _____

in Via _____

cod.fisc. _____

qui di seguito identificata, anche, con il termine "*interessato*" nel significato di cui alla lettera "i" dell'art.4 D.Lgs.n.196/03 e cioè di: "*persona fisica, persona giuridica, ente o associazione cui si riferiscono i dati personali*".

P R E M E S S O

1. Che secondo quanto previsto dall'articolo 23 ("*Consenso*") del D.Lgs.n.196/03 il trattamento dei dati personali da parte di privati è ammesso solo con il consenso espresso dell'interessato fornito liberamente e con specifico riferimento ad un trattamento individuato, oltre che documentato per iscritto e preceduto dall'informativa di cui all'articolo 13 D.Lgs.n.196/03.

2. Che, sempre a norma dell'articolo 23 ("*Consenso*") del D.Lgs.n.196/03 qualora il trattamento riguardi anche, o soltanto, dati c.d. "sensibili" il consenso deve essere manifestato in forma

scritta tranne nelle ipotesi di cui all'art.26 comma 4 lettera "c" il cui contenuto dichiaro di conoscere ed il cui testo riconosco essere quello riportato alla **nota 1** posta in calce alla presente autorizzazione.

3. Che, in ottemperanza al disposto normativo di cui all'articolo 13 ("*Informativa*") del D.Lgs.n.196/03, il cui contenuto dichiaro di conoscere ed il cui testo integrale riconosco essere quello riportato alla **nota 2** posta in calce alla presente autorizzazione, dichiaro di essere stato/a previamente informato/a di quanto segue:

a) I dati personali – identificativi - sensibili e giudiziari (il cui rispettivo significato mi è stato illustrato e riconosco essere quello riportato alla **nota 3** posta in calce alla presente autorizzazione), eventualmente acquisiti, anche, presso terzi, saranno utilizzati – nel rispetto della normativa vigente e fermi gli obblighi di riservatezza e di segreto professionale - esclusivamente per finalità di tipo legale / giudiziario in conformità allo scopo per cui conferisco mandato e, comunque, per finalità connesse e/o strumentali allo svolgimento degli incarichi professionali affidati agli scriventi, escluso – pertanto – ogni utilizzo diverso e/o confliggente con gli interessi del Cliente ("*interessato*").

b) Il conferimento dei dati personali – identificativi - sensibili e giudiziari deve intendersi quale mera facoltà e non obbligo.

c) In mancanza di conferimento dei dati succitati il mandato ed in generale gli incarichi e/o prestazioni professionali richieste – oltre che la prosecuzione di quelli/e in corso - potranno non essere accettati e/o continuati e, dunque, espletati.

d) Qualora venisse autorizzato il trattamento dei dati personali – identificativi - sensibili e giudiziari, questi, nell'espletamento del mandato e/o dell'incarico professionale conferito e, comunque, nei limiti e per le finalità del punto "a" che precede, 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 avvocati titolari, dagli eventuali responsabili e/o incaricati designati (le cui funzioni mi sono state specificate e riconosco essere quelle riportate alla **nota 4** posta in calce alla presente autorizzazione), oltre che dai collaboratori di studio, dai praticanti e dalle segretarie che potranno trattare i dati personali dei Clienti ("*interessati*") anche ai fini della redazione delle note spese. Per l'individuazione delle misure di sicurezza adottate e gli eventuali aggiornamenti e/o modificazioni dei dati identificativi dei titolari, dei responsabili e/o degli incaricati – oltre che, per quanto concerne quest'ultimo aspetto, ai successivi punti "f" e "g" - si fa riferimento al D.P.S. (documento programmatico sicurezza) redatto, cui si rinvia.

e) In caso di sottoscrizione di autorizzazione al trattamento dei dati, all'interessato saranno garantiti tutti i diritti così come meglio specificati all'art.7 ("*Diritto di accesso ai dati personali ed altri diritti* ") D.Lgs.n.196/03 il cui contenuto dichiaro di conoscere ed il cui testo integrale riconosco essere quello riportato alla **nota 5** in calce alla presente autorizzazione.

f) Gli estremi identificativi dei titolari del trattamento sono:

- Avv. _____, nato il _____a _____, cod.fisc. _____;
- Avv. _____, nato il _____a _____, cod.fisc. _____;
- Avv. _____, nato il _____a _____, cod.fisc. _____;

g) Inoltre si segnala pure che:

- ai sensi dell'articolo 4 lettera "g" quale "*responsabile del trattamento*" è nominato il Sig. _____ ; ogni modificazione del nominativo del responsabile verrà comunicata.

  Si fa rinvio al D.P.S. per i nominativi della ditta di assistenza software e hardware dei sistemi informatici dello studio nonché dello studio di commercialisti, cui saranno comunicati i dati personali al solo fine di far fronte ai necessari adempimenti fiscali.

4. che, qualora venisse autorizzato il trattamento dei dati personali – identificativi - sensibili e giudiziari, questi, nell'espletamento del mandato conferito e salvo quanto previsto nel successivo punto 6, nei limiti di legge così come stabiliti ex art.25 D.Lgs.n.196/03 il cui contenuto dichiaro di conoscere ed il cui testo riconosco essere quello riportato alla **nota 6** posta in calce alla presente autorizzazione, nonché per le finalità di cui al punto "a", potranno essere soggetti, oltre che a trattamento, anche a comunicazione e/o diffusione nel significato tecnico così come meglio illustrato alle lettere "a", "l" ed "m" del comma 1 dell'art.4 D.Lgs.n.196/03 e che riconosco essere quello di cui alla **nota 7** posta in calce alla presente autorizzazione.

5. 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.

6. I dati e la documentazione necessari e pertinenti agli incarichi in corso da instaurare o cessati, verranno conservati, in archiviazione, oltre l'esecuzione degli incarichi affidati e precisamente per il periodo di 10 anni.

7. I dati trattati attraverso strumenti automatizzati saranno invece cancellati all'esaurimento dell'incarico conferito, tranne quelli pertinenti e non eccedenti rispetto a successivi incarichi conferiti dal medesimo cliente ("*interessato*").

8. Si fa presente che è facoltà dell'interessato ex articolo 52 D.Lgs.n.196/2003 chiedere – secondo le modalità ed i termini in quella stessa norma indicati - che, per motivi legittimi, sia omessa l'indicazione delle generalità e di altri dati identificativi dello stesso nell'ipotesi di diffusione della eventuale sentenza o di altro provvedimento giurisdizionale.

9. Qualora la presente autorizzazione al trattamento dei dati personali – identificativi - sensibili e giudiziari, dovesse essere sottoscritta l'informativa in essa contenuta dovrà ritenersi valida anche per le posizioni aperte prima del 01.01.2004.

Tutto quanto sopra premesso

SPONTANEAMENTE DICHIARO

di autorizzare, in conformità a quanto sopra indicato e più in generale secondo quanto previsto ex D.Lgs.n.169/03, il trattamento dei miei dati personali di qualsiasi natura ivi compresi quelli c.d. sensibili, identificativi e giudiziari, specificando – altresì – che per l'eventuale fase giudiziale verrà rilasciato apposito mandato nelle forme di legge.

Verona lì _____

F.to
L'INTERESSATO

1. ART.26 comma 4 lettera "c" – GARANZIE PER I DATI SENSIBILI: "[…] **4.** *I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:* ***c)*** *quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397, o – comunque - per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale il diritto 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* […]".

2. ART.13 - INFORMATIVA: "***1.*** *L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente infirmati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) i diritti di cui all'articolo 7; f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art.7 è indicato tale responsabile.* ***2.*** *L'informativa di cui al comma 1 contiene ance gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento da parte di un soggetto pubblico di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.* ***3.*** *Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.* ***4.*** *Se i dati personali non sono raccolti presso l'interessato l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando,è prevista la loro comunicazione, non oltre la prima comunicazione.* ***5.*** *La disposizione di cui al comma 4 non si applica quando: a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla legge comunitaria; b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000 n.397 o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento; c) l'informativa all'interessato comporta un impiego di mezzi che il Garante – prescrivendo eventuali misure appropriate – dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli – a giudizio del Garante – impossibile*".

3. ART.4 – DEFINIZIONI: "[…] ***b) <dato personale>****, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;* ***c)*** *<**dati identificativi**> i dati personali che permettono l'identificazione diretta dell'interessato;* ***d)*** *<**dati sensibili**>, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;* ***e)*** *<**dati giudiziari**>, i dati personali idonei a rivelare provvedimenti di cui all'art.3 comma 1, lettere da a) ad o) e da r) ad u) del D.P.R. 14.11.2002 n.313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61del codice di procedura penale*".

4. ART.4 – DEFINIZIONI: "[…] ***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 ente, 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 responsabile*".

5. ART.7 – DIRITTO DI ACCESSO AI DATI PERSONALI ED ALTRI DIRITTI: "***1.*** *L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la loro comunicazione in forma intelligibile.* ***2.*** *L'interessato ha diritto di ottenere l'indicazione: a) dell''origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art.5 comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.* ***3.*** *L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero - quando via ha interesse – l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere da "a" a "b" sono state portate a conoscenza anche per quanto riguarda l loro contenuto di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.* ***4.*** *L'interessato ha diritto di opporsi in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al*

trattamento dei dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale".
6. ART.25 – DIVIETI DI COMUNICAZIONE e DIFFUSIONE: "**1.** *La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'Autorità giudiziaria: a) in riferimento ai dati personali dei quali è stata ordinata la cancellazione, ovvero quanto è decorso il periodo di tempo indicato nell'art.11 comma 1, lettera "e"; b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.* ***2.*** *È fatta salva la comunicazione o diffusione di dati richiesti, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza da altri soggetti pubblici ai sensi dell'art.58, comma 2, per finalità di difesa o sicurezza dello Stato o di prevenzione, accertamento o repressione di reati*".
7. ART.4 – DEFINIZIONI: "[…] ***a)*** <***trattamento***> *qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati anche se non registrati in una banca dati* […]; ***l)*** <***comunicazione***> *il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati in qualunque forma, anche mediante la loro messa a disposizione o consultazione;* ***m)*** <***diffusione***> *il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione*".

IN OTTEMPERANZA A QUANTO DICHIARATO AI PUNTI "2" e "3" ALLE LETTERE "a", "d" ed "e" OLTRE CHE AL PUNTO "4", **PER PRESA VISIONE** DI QUANTO RAPPRESENTATO ALLE NOTE DA 1 A 7 COMPRESE CHE PRECEDONO,

F.to
L'INTERESSATO

Io ho finito e Vi ringrazio per l'attenzione.

Avv. Andrea Turco
Viale della Repubblica n.6
37126 VERONA
Tel. 045 – 8303031 / Fax. 045 – 8388268
e-mail: aturco@avvocatiassociati.info

Con il patrocinio dell'Ordine degli Avvocati di Verona
Con il patrocinio del Consiglio e Collegio Notarile di Verona

Incontro sul tema

Privacy e studi legali
Misure di sicurezza, Consenso ed Informativa, Il Documento Programmatico

Verona 27 febbraio 2004 ore 15,30

DEONTOLOGIA DEI RAPPORTI AVVOCATO - CLIENTE E PRIVACY.

Cenni di riferimento ai doveri d'informativa e di acquisizione del consenso: D.Lgs.196/2003

***AVV. GIANNANTONIO DANIELI** **

Deontologia e privacy è un tema che porta in un settore della professione forense, ove la norma nasce dalla concreta, quotidiana, esperienza e quotidianamente si evolve, ove i contorni precettivi non sono strettamente marcati e richiedono, per l'interpretazione e l'applicazione, l'intervento ausiliare dell'etica.

La codificazione deontologica è recente, frutto del lungo impegno profuso dal C.N.F. ad adeguatamente porre in iscritto quanto appartiene, o dovrebbe sempre appartenere, al quotidiano professionale, ed anche non, dell'Avvocato; opera realizzata con l'essenziale ricorso ai precedenti della propria giurisprudenza – formatasi, nel tempo, con l'applicazione ai casi concreti dei generali divieti di commettere abusi o mancanze e dei generalissimi precetti di dignità e decoro, sanciti dall'art. 38 L.P.F. - ed ai contributi degli Ordini territoriali (Verona ha partecipato attivamente, con particolare riferimento alla riformulazione dell'art. 17).

Dopo il rigore – per i temi e le competenze delle trattazioni – delle relazioni di Coloro che mi hanno preceduto, confido, quindi, di venir a Voi con considerazioni che possano risultare il meno "volatili" possibile.

La Deontologia Forense ha uno dei suoi pilastri fondamentali nella tutela della riservatezza del rapporto Avvocato - cliente; riservatezza che giunge ad estendersi ai singoli rapporti professionali tra Avvocati, quando l'oggetto ne sia costituito da notizie o proposte che concernano i fatti del cliente dell'uno o dell'altro (l'art. 28 C.D.F. vieta la

produzione di corrispondenza “riservata” tra Avvocati, giungendo, in certo qual senso, a comprimere l’esercizio del diritto di difesa da parte del destinatario).

La riservatezza è un corollario del generale principio di fedeltà nello svolgimento della funzione difensiva, nei rapporti con la parte assistita (rapporti anche preliminari e collaterali allo svolgimento di tale funzione), e nella condotta da tenersi dall’avvocato anche successivamente all’esaurimento del mandato (art. 9, I).

L’origine del dovere di fedeltà – riservatezza, si trae, in linea di principio, dall’essenziale fiduciarietà del rapporto Avvocato - cliente sancita dall’art. 35 C.D.F. e dal rango che l’art. 24 della Costituzione conferisce al diritto di difesa, e quindi, alla funzione defensionale tecnica: diritto di difendersi è anche diritto di scegliersi il difensore (e la recente normativa sul patrocinio a spese dello Stato per i non abbienti, sia in sede civile che penale, costituisce un’attuazione da tempo attesa, anche se non del tutto esaustiva, di tale diritto costituzionale).

La fiduciarietà del rapporto Avvocato - cliente assume, quindi, rango primariamente qualificato nell’ordinamento: il *nemo tenetur se detegere,* nella versione attiva del diritto a difendersi, il diritto, parimenti costituzionale, di agire a tutela dei propri diritti ed interessi legittimi, dal momento in cui vengono posti dalla fiducia e dall’affidamento del cliente nello mani del difensore, impongono a quest’ultimo il sacrale, prima che giuridico, vincolo a tener riservato quanto tra di loro intercorre con riferimento alla trattazione di ciò che è oggetto del mandato difensivo.

In sintesi: il rispetto di tale vincolo da parte dell’Avvocato costituisce condizione imprescindibile per la realizzazione del diritto costituzionale del Cittadino a difendersi.

I secoli di storia, e di vita, dell’Avvocatura italiana, hanno elaborato, ancor prima del Costituente, e fatto entrare ad elemento costitutivo del D.N.A. della categoria forense, questi principi che solo recentemente hanno trovato una certa qual cristallizzazione normativa nel Codice Deontologico Forense del 1997, modificato per alcuni aspetti esemplificativi nel 1999 e nel 2002 (la disposizione finale dell’art. 60 precisa, se ce ne fosse bisogno, che i singoli precetti costituiscono esemplificazioni dei comportamenti più ricorrenti e non limitano l’ambito di applicazione dei principi generali) .

Già nel Preambolo del Codice si afferma che l’Avvocato garantisce il diritto alla libertà e sicurezza e l’inviolabilità della difesa.

Inviolabilità: non solamente da attacchi che possono venire dall’esterno, ma da menomazioni che possano ingenerarsi all’interno del rapporto difensore-cliente.

Passando il Codice si avverte un crescere d'intensità ed un progressivo avvicinamento del precetto di riservatezza al centro della sfera etica dell'Avvocato: partendo dal suo comportamento in costanza di mandato, transitando al comportamento che deve tenere pur a mandato esaurito, pervenendo a por dei limiti alla tutela di suoi pur legittimi interessi (art. 9).

Un breve excursus delle norme:

- l'**art. 6**: impone il dovere di lealtà (profilo interiore - morale della condotta) e di correttezza (profilo pratico - operativo). Considerato *ex parte clientis* evidenzia immediatamente, tra l'altro, la fedeltà e la conseguente riservatezza cui l'Avvocato è tenuto.
- L'**art. 7** (dovere di fedeltà) sotto il profilo in esame non richiede ulteriori appunti.
- **Art. 9**: dovere di segretezza e riservatezza. Concerne l'attività e tutte le informazioni che gli siano fornite dalla parte assistita o di cui sia venuto a conoscenza in dipendenza del mandato.

  > Si mantiene nei confronti degli ex clienti;

  > si estende a favore di chi si rivolge all'Avvocato, senza che il mandato sia da questi accettato.

  Il rispetto di tale dovere dev'essere imposto a > collaboratori > dipendenti > ogni altro soggetto che comunque cooperi all'espletamento dell'attività professionale.

  Le eccezioni sono rigidamente determinate. In linea di principio poste nell'interesse della parte assistita o di primari interessi dell'Ordinamento. Per quanto direttamente lo concerne, l'Avvocato può derogare al dovere di segretezza-riservatezza solamente
- al fine di allegare circostanze di fatto in una controversia (non in una "polemica") nella quale si veda contrapposto l' (ex) assistito;
- in un procedimento concernente le modalità della difesa degli interessi dell'assistito (si pongano le ipotesi di una causa intentata contro l'Avvocato ove sia addotta la sua responsabilità professionale; o di un procedimento disciplinare nel quale siano in questione i suoi rapporti col cliente).

  In ogni caso: la divulgazione delle informazioni concernenti la parte assistita, nei casi sopra indicati, va limitata a quanto strettamente necessario per il fine tutelato.
- L'**Art. 28** pone i divieti di:

- produrre corrispondenza tra colleghi che sia in sé riservata (proposte transattive) o, comunque, qualificata esplicitamente dal mittente come riservata (anche se ciò possa pregiudicare o limitare il diritto di difesa della parte assistita dall'Avvocato destinatario)
- di consegnare al cliente la corrispondenza riservata ricevuta da colleghi;

Come si può vedere, il dovere di riservatezza qui si estende all' Avvocato che assiste la controparte, che può essere portatrice di interessi del tutto opposti al suo mantenimento.

Sarebbe, comunque, interessante esaminare partitamene la pluralità di valori che il principio codificato dall'art. 28 tutela. Ci sarà, spero, altra occasione per farlo.

- **Art. 37**: conflitto d'interessi. L'avvocato deve astenersi dal prestare la propria attività professionale quando questa determini in conflitto con gli interessi di un proprio assistito o interferisca con l'esecuzione di un incarico anche non professionale.

Le ipotesi che qui ci possono interessare sono quelle previste dal canone I:

- il conflitto sussiste non solo nel caso, evidente, che l'espletamento di un nuovo incarico determini la violazione del segreto professionale relativo al rapporto con altro assistito;

ma, altresì, negli ulteriori in cui in cui:

- la conoscenza pregressa degli affari di una parte possa avvantaggiare ingiustamente un nuovo assistito;
- un precedente mandato limiti l'indipendenza nello svolgimento di uno nuovo.
- **Art. 51**: assunzione di incarichi contro ex clienti. E' consentita solamente, tra l'altro, quando vi sia estraneità d'oggetto tra il precedente ed il nuovo mandato e, comunque, non sussista nemmeno l'oggettiva possibilità di far uso di notizie acquisite in ragione del precedente mandato.

Su tali premesse si può vedere come nella sostanza la deontologia forense ben risponda alla *ratio* ed alle esigenze di protezione del cliente tutelate dal Decreto Legislativo:

>> Il dovere d'informare il cliente e di consentirgli l'esercizio dei suoi correlativi diritti, non è che un'espressione, e corollario, della fiduciarietà del rapporto e di tutto quanto ne consegue

>> Il dovere di acquisirne l'autorizzazione al trattamento dei dati: è presunto dal dovere di lealtà e correttezza. L'autorizzazione dell'assistito è una necessaria conseguenza della fiduciarietà del rapporto e, correlativamente, del dovere di segretezza – riservatezza che vincola l'Avvocato.

In linea di principio si può quindi dire che il rispetto della Deontologia da parte dell'Avvocato pone l'assistito al sicuro da ogni abuso sulle informazioni che concernono l'assistito stesso ed i suoi affari.

Il D. Lgs., però, ci impone specifici e formali obblighi:

- all'art. 13, di informare l'assistito sulle finalità e modalità del trattamento dei dati che lo stesso ci fornisce;
- all'art. 23, di chiedere il suo previo il consenso al trattamento dei dati ("il trattamento è ammesso solo con il consenso dell'interessato");

prevede, poi, lo stesso Decreto, la sanzione:

- **penale** (art. 167: 6 – 18 / 24 mesi di reclusione, con riferimento a due diverse ipotesi di "trattamento" non consentito) per la violazione dell'art. 23.

  >> Una tale imputazione a carico dell'Avvocato, richiamerebbe immediatamente l'art. 5,I del C.D.F. che, a sua volta richiamandosi ai generalissimi principi di probità, dignità e decoro, stabilisce l'obbligatorietà dell'azione disciplinare a carico dell'Avvocato "cui sia imputabile un comportamento non colposo che abbia violato la legge penale". E' ben vero che lo stesso canone fa salva l'autonomia della valutazione disciplinare rispetto a quella penale, per cui la prima può divergere dalla seconda; rimane, comunque, l'inderogabilità dell'azione disciplinare.
- Solamente **amministrativa** (art. 161) per la violazione dell'art. 13. Non va, però, omesso di considerare che l'art. 165 dà al Garante la facoltà di applicare anche la sanzione accessoria della pubblicazione dell'ordinanza - ingiunzione su uno o più giornali: è, quindi, da vedere se la pubblicazione (appunto, di una sanzione comminata all'Avvocato, per la violazione di un obbligo postogli dalla legge verso un cliente), possa riflettersi sulla di lui "reputazione professionale" o, comunque, possa compromettere "l'immagine della classe forense". La risposta positiva, renderebbe operativa la previsione sanzionatoria del canone II , art. 5 C.D.F.

Un'osservazione sull'ipotesi penale (trattamento dei dati senza consenso): richiedendo il dolo specifico del profitto proprio od altrui, e la condizione del nocumento, mi auguro sarà di "impossibile" realizzazione da parte di un Avvocato. L'ipotetico e denegato professionista forense che se ne dovesse ritener responsabile, si vedrebbe contestate in sede disciplinare la violazione di tutte le norme deontologiche esaminate, che lo porterebbe, ritengo, a certa radiazione dall'Albo.

Delle autorizzazioni generali che sono state rilasciate del Garante ai liberi professionisti iscritti agli Albi, per il trattamento dei dati dei clienti, ha trattato l'Avv. Bonanno nel suo esauriente e brillante intervento. Per quanto mi concerne, voglio solo evidenziare che con questi provvedimenti è stato formalmente riconosciuto quanto prima dicevo: già la deontologia professionale costituisce valida garanzia contro possibili abusi.

Volendo, comunque prescindere da queste, sotto il profilo disciplinare (e, come abbiamo considerato, prima ancora, amministrativo e penale) va osservato che

- l'art. 13, co. 5, lett b, del Decreto esclude dall'obbligo della previa informazione l'attività giudiziale. Ne rimarrebbe, a rigor di norma, vincolata l'attività stragiudiziale.
- l'art. 24, alla lett. f, afferma che il consenso al trattamento non è richiesto per l'impiego dei dati nell'attività giudiziale.

  Ne esclude, parimenti, la necessità quando il trattamento è necessario per adempiere ad un contratto al quale la parte è interessata (lett. b): è anche il caso dell'Avvocato, che è stretto al cliente dal vincolo del mandato professionale cui deve adempiere.

  Tale seconda scriminante pare costituire una sorta di ripetizione per quanto concerne l'attività giudiziale; assolve, comunque, in via primaria ed esclusiva, dall'obbligo della previa acquisizione del consenso al trattamento dei dati, l'attività stragiudiziale. Con riferimento a quest'ultima, non va, peraltro, dimenticato che si suddivide in attività d'assistenza ed attività di mera consulenza e, forse, tale distinzione porta a diverse conclusioni, per l'una e per l'altra. Invero:

  - l'assistenza si inserisce nella contrapposizione o, comunque, nel confronto, fra due o più parti. L'Avvocato agisce, in rappresentanza e difesa di una di

queste, su mandato della stessa. Il contratto di mandato è solo presuntivamente oneroso (1709 C.C.), ben può essere convenuta la gratuità della prestazione professionale ed anche in tale ipotesi l'Avvocato agisce in forza di vincolo contrattuale con l'assistito.

- Per quanto concerne la consulenza stragiudiziale, osservo che quando questa si svolge su base contrattuale (d'opera intellettuale, artt. 222 e segg. C.C.) rientra nell'ipotesi della lett. b dell'art. 24 e, pertanto, il trattamento dei dati che la stessa richiede non è soggetto a previa autorizzazione dell'interessato. Detta autorizzazione parrebbe, invece, necessaria per la consulenza gratuita (prestata per volontariato sociale, o ad amici, parenti *et similibus* – ammessa in sede deontologica) che non si fonda su contratto d'opera (sinallagmatico), oneroso per il cliente.

Conclusivamente, per quanto traggo da una prima, spero non azzardata o sconsiderata lettura, il D. Lgv. può comportare rischi di sanzioni disciplinari
nei casi di difetto:

- d'informativa nelle prestazioni stragiudiziali (5, II, C.D.F.);
- di previa acquisizione del consenso al trattamento, nelle prestazioni gratuite di consulenza stragiudiziale (5, I); nella ricorrenza, ovviamente, di tutti i requisiti necessari ad integrare l'ipotesi penale dell'art. 167 del Decreto.

Ho messo le mani avanti, nel proporre le considerazioni conclusive; in effetti, pur risultandomi rigorose, evidenziano (autorizzazioni del Garante a parte) aspetti e conseguenze sconcertanti per la sede disciplinare.
Prendete il tutto solamente quale iniziale stimolo, forse provocatorio, per la riflessione e l'approfondimento.

Confidiamo, del resto, tutti, che il Garante adempia al più presto all'onere postogli dall'art. 12 del Decreto, di promuovere la formazione di quei codici di "deontologia e buona condotta", che dovrebbero servire, per ogni singola categoria, a chiarire gli aspetti bui o incongrui delle normativa e a sviluppare adeguate ed inequivoche modalità d'esecuzione dei precetti che questa pone.

Per parte nostra, attiveremo su questo tema la Commissione per la Deontologia dell'Ordine, a fini certamente di studio e di proposta, ma, altresì, per fornir la possibile

consulenza ai Colleghi su questi temi.

Esula dal tema affidatomi, ma non va qui sottaciuto che l'Avvocato non può, anche sotto il profilo deontologico, legittimamente omettere di adottare le misure minime per la corretta conservazione dei dati concernenti i clienti e la loro protezione da intromissioni ed abusi di terzi; adempimenti che, a nostro opportuno aggiornamento, sono stati puntualmente ed esaurientemente illustrati dalle relazioni degli Avvocati Rosa, Giacopuzzi e Ferrarese.

Non pare, invero, difficile considerare che l'adozione di tali misure, ritenute oramai necessarie anche per comune esperienza professionale, corrisponda alla necessaria osservanza dei precetti, oltre che di riservatezza, di correttezza nei rapporti col cliente; che deve poter supporre che l'Avvocato si attenga, tra l'altro, a tutto quanto l'ordinamento gli prescrive a tutela del diritto alla riservatezza di colui che assiste.

***** *del Foro di Verona.*
Coordinatore della Commissione dell'Ordine per la Deontologia

E mail: danieli@veronalex.it

N.B.: Purtroppo non ci è giunta ancora la relazione del Dr. Aldo Celentano, ma l'approssimarsi del 31 marzo ci induce alla pubblicazione degli atti, con l'impegno di diffondere il testo dell'intervento mancante non appena in nostro possesso.
Attendiamo ovviamente ogni utile suggerimento ed integrazione che i Colleghi vorranno farci pervenire.

Avv.to Luca Venturini

Prima della pubblicazione degli atti è apparsa la notizia che vi riportiamo, citandone la fonte:
"03 Marzo 2004 ***- Obbligatorio segnalare al garante la banca dati dei clienti***
L'interpretazione dell'articolo 37, lettera f), del codice della privacy obbliga a notificare e rinotificare i trattamenti di dati gestiti con strumenti elettronici relativi all'adempimento di obbligazioni. Rientra in questa categoria per esempio la banca dati clienti, gestita da un'impresa al fine di verificare se sono state onorate le fatture o comunque pagati i corrispettivi. L'ampia formulazione della citata lettera f) in mancanza di interpretazioni ufficiali del garante obbliga le categorie economiche ad attrezzarsi per predisporre la notificazione. L'articolo 163 del codice della privacy prevede una pena pecuniaria da 10 mila a 60 mila euro. (Fonte: Italia Oggi) "