Il trattamento dei dati personali all'interno dello studio

Avv. Jacopo Bandinelli

I soggetti – il titolare

- Titolare del trattamento è il soggetto a cui spettano le decisioni di fondo in ordine a finalità, modalità e strumenti utilizzati, ivi compresa la sicurezza
- Attività prestata singolarmente: titolare è la persona fisica dell'avvocato esercente; se sono congiuntamente più professionisti, sono contitolari del trattamento
- Attività svolta da una società di professionisti o associazione professionale: titolare è l'entità nel suo complesso

I soggetti – il responsabile

Figura “eventuale”: il Titolare, con un atto scritto nel quale vanno indicati i compiti affidati, può nominare un Responsabile del trattamento che può essere anche estraneo alla struttura.

I soggetti – il responsabile

- La scelta deve cadere su persone fisiche od organismi che per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Nella società o associazione professionale possono essere i singoli professionisti soci, ad es. ciascuno per il trattamento dei dati dei propri clienti.

I soggetti – gli incaricati

- Tutte le persone fisiche che hanno acccesso ai dati a vario titolo (avvocati, praticanti, collaboratori, personale amministrativo).

- Il titolare deve individuare per iscritto l'ambito del trattamento consentito: è consentito utilizzare le modalità semplificate per le istruzioni agli incaricati (scritto unico con istruzioni precise e chiare e tutti gli incaricati).

Art. 31 - Obblighi di sicurezza.

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.

Obblighi specifici sui dati personali

- Custodia e controllo
  - per finalità di riduzione al minimo dei rischi
    - di distruzione o perdita
    - di accesso non autorizzato
    - di trattamento non consentito
    - di trattamento non conforme alle finalità della raccolta

Art. 33 – Misure minime

Nel quadro dei più generali obblighi di cui dall'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo [...] volte ad assicurare un livello minimo di protezione dei dati personali

Art 31

- Detta gli obblighi generali di sicurezza
- Indica le finalità da perseguire in modo tendenziale
- Fonda la responsabilità civile

Art. 33

- Indica le misure minime da adottare in ogni caso
- La sua mancata applicazione è causa di responsabilità penale

Misure minime di sicurezza

Trattamenti senza l'ausilio di strumenti elettronici (art. 35)

- periodico aggiornamento degli ambiti dei trattamenti consentiti ai singoli incaricati
- previsione di procedure di idonea custodia degli atti e documenti affidati agli incaricati
- conservazione di atti e documenti in archivi ad accesso selezionato
- disciplina delle modalità di accesso agli archivi

Misure minime di sicurezza

Trattamenti con strumenti elettronici (art. 34)

- autenticazione informatica
- procedure di gestione delle credenziali di autenticazione
- sistema di autorizzazione
- aggiornamento dell'individuazione dei trattamenti consentiti ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici

Misure minime di sicurezza

(*Segue*) Trattamenti con strumenti elettronici (art. 34)

- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- tenuta di un aggiornato documento programmatico sulla sicurezza

Misure minime di sicurezza

L'allegato B del Codice costituisce il disciplinare tecnico per l'adozione delle misure minime di sicurezza.

Indica analiticamente i modi di adozione delle misure minime di sicurezza

Distingue le misure di sicurezza in relazione al tipo di trattamento ed ai dati trattati

Allegato B
Trattamenti non elettronici

- Istruzioni scritte in ordine al controllo ed alla custodia dei dati
- Individuazione dell'ambito di trattamento consentito ai singoli incaricati o a classi omogenee di essi (lista degli incaricati)
- aggiornamento almeno annuale della lista degli incaricati
- eventuale redazione della lista degli incaricati per classi omogenee di autorizzazione

Allegato B
Trattamenti non elettronici

- Trattamento di dati sensibili o giudiziari: obbligo di custodia da parte degli incaricati durante la lavorazione
- Obbligo di controllo degli archivi contenenti dati sensibili o giudiziari (con sistema elettronico di controllo accessi o con preventiva autorizzazione)
- Identificazione e registrazione di chi accede agli archivi dopo la chiusura

Autenticazione informatica

- Ciascun incaricato deve possedere la propria credenziale di autenticazione
- Il trattamento è consentito agli incaricati dotati di credenziali dopo il superamento di una procedura di autenticazione per un insieme specifico di trattamenti
- Obbligo di segretezza delle credenziali di autenticazione

La parola chiave

- La password deve essere di almeno otto caratteri (o, se minore, il massimo consentito dal sistema operativo)
- Non deve contenere riferimenti facilmente riconducibili all'incaricato (nome, data di nascita...)
- Ciascun incaricato la modifica al primo utilizzo
- Viene modificata ogni 6 mesi (3 mesi per trattamenti di dati sensibili o giudiziari)

La parola chiave

La parola chiave deve essere disattivata:

- dopo 6 mesi di mancato utilizzo
- in caso di perdita della qualità che consente all'incaricato l'accesso ai dati

E se l'incaricato va in ferie?

Regole per rendere comunque possibile l'accesso ai dati anche in assenza dell'incaricato

- istruzioni preventive e scritte
- sulle modalità con cui il titolare può accedere ai dati
- per necessità indifferibili di operatività e sicurezza
- con individuazione preventiva dei soggetti che custodiscono le copie delle credenziali

Profili di autorizzazione

L'autenticazione è un sistema che permette l'identificazione del soggetto che effettua i trattamenti

L'autorizzazione è un sistema che consente a ciascun incaricato l'accesso esclusivamente ai dati che egli deve trattare

Profili di autorizzazione

- sono previsti per classi omogenee di ‘incaricati’ (es: incaricati della contabilità accedono solo ai dati identificativi e fiscali dei clienti)
- sono individuati e configurati prima dell'inizio del trattamento
- sono aggiornati almeno una volta all'anno

Altre misure minime

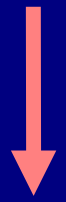
- Elaborazione ed aggiornamento almeno annuale della lista degli incaricati e addetti alla gestione e manutenzione degli strumenti elettronici (sovente si tratta di organizzazioni esterne allo studio legale)
- Tenuta ed aggiornamento di software antivirus ed antispyware
- Aggiornamento di sicurezza dei software in dotazione
- Salvataggio dei dati con cadenza almeno settimanale

Dati sensibili e giudiziari

- Misure di sicurezza più stringenti
- Protezione contro l'accesso abusivo
- Istruzioni sull'uso e la custodia dei supporti rimovibili contenenti i dati
- distruzione dei supporti rimovibili dopo l'uso o cancellazione dei dati contenuti
- procedure di *disaster recovery* dei dati per consentirne il ripristino entro 7 giorni

Il DPS

La redazione del Documento Programmatico sulla Sicurezza è essa stessa una misura di sicurezza



La sicurezza dei dati si ottiene solo mediante l'adozione e l'aggiornamento di procedure di sicurezza

Il DPS: solo per i dati sensibili?

L'allegato B (n. 19) sembra stabilire l'obbligo del DPS solo per i trattamenti di dati sensibili e giudiziari

Tuttavia un'interpretazione più corretta impone di considerare obbligatorio il DPS per tutte le tipologie di dati trattati in forma elettronica

Il DPS: per tutti i dati

- L'obbligo per tutti i dati è sancito dall'art. 34 del Codice
- La previsione di cui al punto 19.7 dell'allegato B costituirebbe un'ingiustificata disparità di trattamento
- Non si comprenderebbe la necessità di uno specifico paragrafo sulle "*ulteriori misure di sicurezza*" per il trattamento dei dati sensibili e giudiziari

Il DPS: contenuti

- Il DPS è un documento di analisi della situazione e di programma delle attività da svolgere.
- Il DPS contiene la descrizione di procedure da mettere in atto a fronte di eventi futuri e possibili.

Analisi dei rischi

Devono essere individuati i rischi che incombono sui dati e di essi deve essere individuato un grado di probabilità di verificazione dell'evento

I rischi dipendono sia da fattori ambientali e fisici, sia da fattori legati all'utilizzo di apparecchiature tecnologiche

Misure da adottare

Occorre mettere in atto misure di protezione dei dati personali che garantiscano:

- l'integrità e la disponibilità dei dati
- la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Misure da adottare: *disaster recovery*

Devono essere adottate misure e procedure per garantire il ripristino dei dati in caso di distruzione o danneggiamento degli stessi.

L'adozione di tali misure e procedure deve consentire di ridurre al minimo i rischi di distruzione o danneggiamento

Disaster recovery: qualche esempio

- Rottura del PC → Backup su disco esterno o su server
- Furto del PC → Backup su disco esterno o su server
- Incendio in studio → Backup su disco fuori dello studio

Obblighi di formazione

- Tutti gli incaricati devono ricevere specifica formazione sui rischi connessi ai trattamenti e sulle misure in essere per ridurre tali rischi, sulle responsabilità che derivano dal trattamento e sui modi per aggiornarsi sulle misure minime
- La formazione deve essere svolta al momento dell'assunzione e, successivamente, ad ogni cambio di mansioni o significativi mutamenti dei sistemi

Trattamenti affidati all'esterno

Devono essere descritti i criteri da adottare per garantire il rispetto delle misure minime sui dati legittimamente trattati all'esterno dello studio

Uno dei criteri possibili è ottenere dall'affidatario comunicazione in cui egli dichiara di aver adottato le misure minime all'interno della sua struttura

Il nuovo codice di deontologia e buona condotta

6 Novembre 2008

G.U. 24 Novembre 2008, n. 275

Entrata in vigore: 1 Gennaio 2009

Il nuovo codice di deontologia e buona condotta

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

Alcune disposizioni

E' prevista l'adozione di speciali cautele per prevenire l'ingiustificata raccolta di dati in caso di:

- scambio di corrispondenza
- esercizio contiguo di attività autonome all'interno di uno studio
- utilizzo di dati su particolari supporti o particolari documenti
- utilizzo di banche dati ad uso interno, in particolare se situate in altre sedi e consultabili in via telematica

Domande