

### ALCUNE INFORMAZIONI UTILI DOMANDE E RISPOSTE

#### A. Quali dati sono da considerarsi personali?

A titolo di esempio si possono indicare:

1. il nome, il cognome, l'indirizzo, il numero di telefono, il codice fiscale, la partita I.V.A., dati bancari...
2. informazioni circa la composizione del nucleo familiare, la professione esercitata da un determinato soggetto, sia fisico che giuridico, la sua formazione...
3. fotografie, radiografie, video, registrazioni, impronte...
4. informazioni relative al profilo creditizio, alla retribuzione...
5. informazioni relative alla salute di un soggetto, alla vita sessuale, alla partecipazione ad associazioni di categoria, a partiti, trattenute sindacali, cartelle cliniche, rilevazioni di presenze...

#### B. Ci sono adempimenti diversi a seconda del soggetto che tratta i dati?

Si, ovviamente una ditta individuale che non si avvale di nessun collaboratore, sarà gravata da pochi adempimenti rispetto ad una struttura societaria.

A seconda della dimensione e della tipologia di struttura che effettua il trattamento dei dati, dal tipo di dati trattati (solo comuni? anche [sensibili](#) o giudiziari?) delle modalità di trattamento, dell'esistenza o meno di una struttura informatica collegata ad internet, gli adempimenti sono differenti.

#### C. Di quali adempimenti si tratta?

Si tratta ad esempio di nominare le figure richieste dalla legge, di proteggere gli elaboratori contro il rischio di intrusione e di virus, di adottare delle misure fisiche di protezione (allarmi, stabilizzatori di corrente, armadi chiusi a chiave ed ignifughi, accesso selezionato ai locali...), di mettere per iscritto le procedure da seguire e soprattutto di redigere il [DPSS \(documento programmatico sulla sicurezza\)](#), una documentazione che descrive quanto fatto in materia di [tutela dei dati personali](#) ed individua quanto ancora resta da fare. Solo il DPS fa prova dell'avvenuto adeguamento alla normativa.

#### D. L'Azienda o lo Studio professionale è obbligato a nominare il Responsabile del Trattamento?

No. L'art. 29 del d. lgs. n. 196/2003 prevede che tale figura sia designata facoltativamente. Per le piccole aziende la nomina di un Responsabile del trattamento appesantisce solamente la struttura e gli oneri degli operatori. In una azienda media, invece, la figura del Responsabile si rende quanto mai necessaria per coordinare la realizzazione degli adempimenti previsti dalla legge e la vigilanza sugli incaricati e sulle misure di sicurezza.

#### E. Come si può fare per evitare di ricevere messaggi pubblicitari indesiderati?

Con la crescita delle reti telematiche si è sviluppato di pari passo anche lo spamming, un fenomeno senz'altro fastidioso.

Le regole di buona educazione stabilite dagli utenti di Internet (norme di Netiquette) vietano lo spamming e, per assicurare l'applicazione di tale regola, la Naming Authority ([www.nic.it](http://www.nic.it)) ha istituito uno spazio presso il proprio sito (<http://www.nic.it/RA/servizi/listserv/abuse.html>) in cui i cittadini privati possono segnalare tutte le violazioni di Netiquette. Una sorta di "lista nera" dello spamming.

Per attivarsi a tale riguardo è necessario segnalare la violazione delle norme di Netiquette alla Naming Authority Italiana e alla Registration Authority Italiana attraverso l'invio di una e-mail a [ABUSE@NA.nic.it](mailto:ABUSE@NA.nic.it). Successivamente la Naming Authority prenderà contatto con i responsabili e loro providers per segnalare la questione e permettere il contraddittorio.

In ogni caso, anche il Codice della privacy vieta l'invio di materiale pubblicitario o di vendita diretta tramite posta elettronica senza il consenso espresso del destinatario (art. 130 del D. Lgs. n. 196/2003). Se poi le comunicazioni promozionali sono camuffate o celano l'identità del mittente o non forniscono un idoneo recapito presso cui esercitare i diritti di cui all'art. 7, si configura un'ipotesi di **illecito penale** previsto dall'art. 167 (**Trattamento illecito di dati**) che contempla una pena che arriva fino a tre anni di reclusione.

### F. Il DPSS deve avere data certa? e come si fa ad adempiere a tale obbligo?

In realtà il Codice della privacy fa riferimento alla data certa solamente quando parla dell'impossibilità del Titolare di adeguare alle misure minime gli strumenti elettronici entro il 31 dicembre (art. 180). Ciò non esclude che, a fini probatori, anche il Documento Programmatico sulla Sicurezza debba essere adottato con data certa: come si riuscirebbe, altrimenti, a dimostrare agli organi di controllo che la misura è stata adottata entro i termini previsti dalla legge?

Il metodo più pratico per dimostrare la certezza della data, per evitare di ricorrere a metodi dispendiosi come la vidimazione presso un notaio di un verbale, è quello dell'**autoprestazione**: apposizione presso un ufficio postale del timbro direttamente sul Documento, nel caso in cui questo sia rilegato in modo non scomponibile; oppure conservandolo in busta chiusa e timbrata.

### G. Quali sono le sanzioni previste dal CODICE DELLA PRIVACY?

Semplifichiamo mediante questo schema:

| Articolo del Codice | Illecito   | Sanzione  |
|---------------------|--|---|
| 161                 | Assenza informativa privacy  | Sanzione amministrativa da 3.000 a 18.000 euro  |
| 161                 | Assenza informativa privacy per dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilevanza del pregiudizio | Sanzione amministrativa da 5.000 a 30.000 euro. (moltiplicabile per 3 a seconda delle condizioni economiche del contravventore)           |
| 163                 | Omessa o incompleta notificazione al Garante   | Sanzione amministrativa da 10.000 a 60.000 euro.  |
| 164                 | Omissione di fornire informazioni o esibire documenti richiesti dal Garante Privacy  | Sanzione amministrativa da 4.000 a 24.000 euro.   |
| 167                 | Trattamento illecito di dati personali   | Possibile estinguere il reato ex art. 169, pagando una somma di denaro se ci si regolarizza entro il termine prescritto (non + di 6 mesi) |
| 168                 | Falsità nelle dichiarazioni e notificazioni al Garante   | Sanzione penale, reclusione da 6 mesi a 3 anni  |
| 169                 | Omessa adozione di misure necessarie alla sicurezza dei dati   | Arresto fino a 2 anni o sanzione amministrativa, pagamento di una somma da 10.000 a 50.000 euro.  |
| 170                 | Inosservanza dei provvedimenti del Garante   | Arresto da 3 mesi a 2 anni.   |

### H. La Formazione del personale addetto è obbligatoria?

Sì, l'articolo 19.6 recita chiaramente che "La previsione di interventi formativi degli incaricati del trattamento,.....", "La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni....."

### I. Sono obbligato ad adeguarmi anche se in ufficio ho solo un NOTEBOOK?

Sì, i computer portatili, sono mezzi informatici.

Altresì riteniamo fare presente che nella stessa categoria generale ovvero "microcomputer" fanno parti anche i cosiddetti computer palmari, laptop, notebook, i "personal organizer", i PDA, ecc. ecc... Tra le altre cose ricordiamo che queste meravigliose ed utile tecnologie sono soggetti sicuramente a rischi maggiori di un Server o un altro elaboratore di dimensioni più grandi, ad esempio sono maggiormente soggetti a furto, smarrimento, utilizzo fuori dall'azienda, ecc. ecc....

### J. Backup e Ripristino dei Dati?

La normativa in merito è abbastanza esauriente, i dettami legislativi li troviamo essenzialmente negli articoli 18 - 19.5 e 23.

Analizzando attentamente il Codice si comprende la necessità di applicare le regole che vengono applicati dagli esperti in sicurezza e disaster recovery, che essenzialmente sono:

- a) redigere una policy che stabilisca gli obiettivi;
- b) identificare i dati/file che vanno "protetti"
- c) identificare le misure di prevenzione ;
- d) sviluppare un piano di recupero
- e) analizzare l'impatto di una situazione di emergenza;
- f) pianificare la prova, l'addestramento e la simulazione del piano adottato

### K. Se ho solo archivi cartacei e non utilizzo PC od altri strumenti informatici?

Chi tratta dati personali senza tali mezzi è tenuto ad adottare le seguenti cautele:

- a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito;
- b) prevedere procedure per la conservazione di determinati atti in archivi ad accesso selezionato
- c) prevedere procedure per un'idonea custodia degli atti affidati agli incaricati per lo svolgimento dei relativi compiti
- d) identificare chi accede ai dati
- e) ecc., ecc..

### L. Che cosa sono gli strumenti elettronici?

La legge dice se sono "Strumenti Elettronici gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento". Pertanto possono essere sicuramente compresi tra gli strumenti elettronici: Computers, cellulari con fotocamera, macchine fotografiche digitali, smart card e tutti gli altri strumenti elettronici che la tecnologia mette a disposizione.

### M. Come sono e cosa sono i DATI PERSONALI?

La legge definisce **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.

La legge definisce **Dato Sensibile**: 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.

La legge definisce **Dati Giudiziari**: I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a 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 61 del codice di procedura penale.

### N. All' articolo 20 si fa riferimento all'Art. 615 ter, cos'è?

L'articolo 615 ter è un articolo del codice penale che recita:

"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. ".....

- In particolari casi sanciti dalla norma la pena può essere elevata sino a 8 anni.

### O. Come si possono proteggere gli strumenti informatici?

Esistono diversi metodi per impedire gli accessi non autorizzati dalla rete internet (naturalmente i fattori che determinano il grado di sicurezza varia secondo i mezzi ed i metodi impiegati).

Uno dei sistemi dal nome noto è l'utilizzo di un Firewall, i firewall possono essere sia hardware sia software (secondo le necessità).

Esistono firewall "commerciali" a costi accessibili e firewall appositamente "costruiti e configurati" secondo l'utilizzo e le necessità dell'utente.

In via esemplificativa il Firewall è un sistema o gruppo di sistemi che attuano un complesso di regole che controllano l'accesso tra due reti.

Maggiori informazioni? **NON ESITATE A CONTATTARCI.**