FAQ

1) **D. Che differenza c'è fra le misure minime di sicurezza e le misure idonee e preventive di sicurezza?**
   R. Le misure minime di sicurezza (art. 33 e allegato B) vanno comunque e sempre adottate, e sono specificate nell'allegato B. La mancata adozione è sanzionata con l'arresto sino a 2 anni o l'ammenda dai 10.000 ai 50.000 euro (art. 169);
   le misure idonee e preventive (art. 31) sono un obbligo più generale, cioè oltre le misure minime di sicurezza vanno adottate anche le misure idonee e preventive per custodire e controllare i dati, 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 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.

2) **D. A cosa serve il Documento Programmatico della Sicurezza (DPS)?**
   R. Il Documento Programmatico per la Sicurezza identifica gli aspetti dell'infrastruttura tecnologica aziendale coinvolti nella gestione di dati personali e sensibili, verificandone l'aderenza a quanto disposto dalle più recenti normative (D. Lgs. n.196 del 30 Giugno 2003). Inoltre, il DPS definisce e descrive le misure necessarie per una vera "messa in sicurezza" del sistema informativo aziendale.

3) **D. Se un utente compila un form e poi preleva un manuale, si possono inviare successivamente email informative?**
   R. Nel momento della compilazione del form, va data l'informativa dell'art. 13 e va richiesto anche il consenso per l'invio di email successive.

4) **D. Il documento è solo un adempimento legale?**
   R. Il documento rappresenta non solo un adempimento legale ma un vero e proprio strumento di riferimento per l'azienda in materia di trattamento dei dati personali, e in generale di definizione delle strategie di sicurezza, e delle conseguenti policy che tutti i dipendenti, collaboratori, partner e fornitori devono adottare.

5) **D. Chi deve compilare il DPS?**
   R. L'obbligo di redazione del DPS (Documento Programmatico sulla Sicurezza) coinvolge tutti i soggetti che trattino dati sensibili o giudiziari con l'ausilio di strumenti elettronici

6) **D. È obbligatorio preparare un D.P.S che contenga un'analisi dei rischi?**
   R. Si, è esplicitamente richiesto dal comma 19.6 dell'Allegato B del D.lgs. 196/2003 per tutte le organizzazione che trattano dati personali, sia essi generici, sensibili o giudiziari con l'ausilio dei strumenti elettronici.

7) **D. Una login e una password, devono essere considerati dati personali?**
   R. Si, in base a quanto definito dall' art.4 del Codice.

8) **D. Può un provider di servizi Internet fornire i dati di un suo cliente a chiunque ne faccia richiesta?**

R. Solo se ha preventivamente e chiaramente informato l'interessato dell'ambito di comunicazione e diffusione dei dati e ne ha acquisito il consenso a tali operazioni.

9) **D. Può un provider essere ritenuto responsabile della violazione da parte di crackers e criminali informatici della password e del user-id di un suo utente, una volta che con i dati violati si commettano atti illegali**

R. Si, se non ha adottato le idonee misure di sicurezza. E' responsabile, peraltro, anche se non si commettono illeciti penali, ma l'interessato subisce un danno dall'uso non autorizzato della sua ID (ad esempio gli viene cancellata la mailbox). Si vedano, a tal proposito, gli artt. 31 e sgg. del Codice della privacy (D. Lgs. n. 196/2003). Il cracker è comunque responsabile ai sensi della legge anticrimini informatici.

10) **D. Vorremo avere chiarimenti sull'applicazione del Codice della Privacy agli internet providers. In particolare, abbiamo l'elenco dei nostri clienti in un database. Questi dati vengono utilizzati per il conteggio del traffico utenti, per le scadenze e per gli avvisi all'utente.Rientriamo fra coloro che devono fare la notifica al Garante?**

R. Se la raccolta è effettuata al fine esclusivo di fornire i servizi richiesti agli utenti e non vi è eccedenza nella raccolta dei dati rispetto alle suddette finalità, non c'e l'obbligo di notificare il trattamento.

11) **D. I dati della mia clientela saranno soggetti alla legge sulla privacy. Come mi dovrò comportare con le trattenute sindacali e relativi versamenti?**

R. Sarà sufficiente ottenere dagli interessati il consenso scritto al trattamento dei loro dati sensibili e fornire una completa informativa, ai sensi dell'art.13 della legge.

12) **D. Un'azienda raccoglie dati di molti corrispondenti (anche persone fisiche), necessari a tenere le normali relazioni commerciali e scritture contabili; non tutti questi dati si possono considerare "pubblici". Sono comunque soggetti al consenso?**

R. E' possibile considerare tali dati come rientranti nell'ambito dello svolgimento di un'attività economica e quindi sottratti al consenso ai sensi dell'art.24 del Codice della privacy.

13) **D. In un'azienda che possiede un archivio interno per la fatturazione ai clienti contenenti dati anagrafici:**

1) Il codice della privacy si applica anche in questi casi?

2) Se si cosa dobbiamo fare?

R. Il trattamento dei dati in questione, in quanto effettuato sulla base di obblighi di legge,o comunque connesso all'adempimento di obbligazioni contrattuali di cui l'interessato è parte, non è soggetto all'obbligo di consenso. Per i dati comuni, in ogni caso, occorre dare l'informativa prevista dall'art.13 e rispettare i principi dell' art.11 del codice.

14) **D. Cosa succede in caso di presenza nelle pagine web di elenchi di rivenditori, distributori, ecc.?**

R. Il contenuto informativo delle pagine è responsabilità dei singoli realizzatori e gestori di pagine web, che dovranno verificare, di volta in volta, se rientrano ed in che misura nell'ambito di applicazione della legge.

Nel caso in cui la cura e la realizzazione tecnica (e non contenutistica) delle pagine fosse a vostro carico, Voi potreste essere considerati, se esiste un preciso incarico scritto in tal senso, responsabili del trattamento, se curate anche aspetti organizzativi complessi (ad esempio, aspetti connessi alla sicurezza delle informazioni); altrimenti, siete esclusivamente incaricati del trattamento, con il compito di "mettere in rete" contenuti informativi sulla base delle precise indicazioni a Voi fornite, sempre per iscritto, dal titolare del trattamento.

15) **D. In quali casi l'informativa è inidonea e quindi soggetta a sanzioni?**

R. L'informativa deve contenere tutti i punti previsti dall'art. 13, e la mancanza di anche uno solo è considerata inidonea informativa, sanzionata dall'art. 161.

16) **D. Quali sono le regole da seguire per chi non tratta dati sensibili o giudiziari?**

R. E' difficile che una organizzazione (azienda, ente, studio professionale) non abbia archivi con dati sensibili: pensiamo per esempio ai certificati di malattia dei dipendenti.

17) **D. Sono un consulente del lavoro: quali sono gli adempimenti relativi alla gestione del personale dipendente / autonomo, della clientela?**

R. Occorre dare l'informativa e raccogliere il consenso per i dati sensibili trattati, nonché rispettare i principi di cui all'art.11 del codice.

Anche per quando riguarda i dati comuni, in mancanza di una nomina a incaricato o a responsabile del trattamento da parte delle aziende che si avvalgono della Sua collaborazione, dovrà provvedere alla raccolta del consenso.

18) **D. Se un cliente invia un ordine con i suoi dati via fax o via web, va messa l'informativa?**

R. Si, non è però necessario il consenso se poi si promuovono servizi analoghi, in base all'art. 130 comma.