Gestione della Privacy

Dal 2004 il **Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"** ha sostituito la Legge n. 675/1996. Le disposizioni legislative prevedono l'applicazione – da parte di tutte le organizzazioni – di procedure più estese rispetto al passato per la tutela dei dati personali, soprattutto quelli gestiti su supporto elettronico.

Il D.Lgs 196/2003 prevede alcuni adempimenti formali quali: la nomina del Titolare e di un Responsabile del trattamento dei dati personali – di capacità tecniche adeguate – la definizione documentata dei compiti assegnati al responsabile del trattamento, la designazione scritta degli incaricati al trattamento dei dati personali, la redazione di istruzioni scritte per definire le modalità di trattamento dei dati personali da parte degli incaricati nominati, la predisposizione facoltativa e l'aggiornamento annuale del Documento Programmatico sulla Sicurezza, la raccolta del consenso degli interessati, ove previsto anche in forma scritta, ecc…

Il D.Lgs 196/2003 prescrive le misure minime di sicurezza che ogni organizzazione che tratti dati personali attraverso sistemi informatici deve adottare, in particolare (si riporta l'art. 34 della Legge, Trattamenti con strumenti elettronici):

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le cosiddette misure minime di sicurezza.

L'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza), descrive chiaramente quali sono gli accorgimenti tecnici da adottare (nome utente, password, antivirus, firewall, ecc.).

Si ricorda che per "dato personale", si intende "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", quindi dati sul personale dipendente e sui collaboratori (schede del personale, dati anagrafici e contabili), dati relativi a fornitori e clienti per i quali non esiste un precedente consenso.

La Legge n. 35 del 04/04/2012 ha eliminato di fatto la necessità di redazione (od aggiornamento) del Documento Programmatico sulla Sicurezza (D.P.S.) da parte di

tutti i tipi di imprese e liberi professionisti, indipendentemente dal tipo di dati trattati.

La sostanza della normativa privacy non è di fatto cambiata con l'abolizione del DPS e rimangono le stesse misure di sicurezza obbligatorie ed i provvedimenti del Garante che hanno effetto di legge (ad es. quello generale sulla videosorveglianza, quello sugli amministratori di sistema, le linee guida del Garante per posta elettronica e internet nei luoghi di lavoro) che, come atti di natura prescrittiva, se non rispettati espongono i contravventori a pesanti sanzioni.

Si precisa che l'entrata in vigore del **nuovo Regolamento europeo sulla protezione dei dati personali (Reg. UE 679/2016),** avvenuta lo scorso **24 maggio 2016**, stabilisce nuove regole nella gestione della privacy a livello europeo, concedendo alle organizzazioni 2 anni di transizione per adeguarsi.

La semplificaziona introdotta negli ultimi anni attraverso l'abolizione della tenuta del DPS, presenta, però, anche l'altra faccia della medaglia, cioè quello di essere indotti – anche a causa della crisi economica – ad "allentare" o addirittura a "mollare" la gestione della privacy aziendale, con il potenziale rischio di rimanere "scottati" al primo imprevisto. La stesura del DPS, tra l'altro, era ritenuto erroneamente da molte organizzazioni una sorta di adeguamento normativo omnicomprensivo sul tema della privacy, mentre invece le dichiarazioni riportate nel DPS non hanno alcun valore se poi non sono messe in pratica.

Ora il nuovo Regolamento Europeo (si veda articolo Nuovo Regolamento UE sulla Privacy) impone alle organizzazioni di ripensare alla gestione della Privacy in un'ottica di valutazione dei rischi e di adozione di misure di sicurezza "adeguate" (non più "minime") da mantenere al passo con l'evoluzione tecnologica delle minacce del cybercrime.

Si ricordi, infine, che i delitti sulla privacy sono entrati a far parte dei reati compresi nel D.Lgs 231/2001 e s.m.i. con pesanti conseguenze per le imprese che dovessero incorrere in tali reati anche solo per omesse misure di sicurezza.

Non essendo più necessario redigere e, soprattutto, aggiornare il DPS a cadenza annuale, le organizzazioni che trattano dati sensibili o giudiziari di persone fisiche (clienti e fornitori) dovranno comunque continuare ad osservare alcune regole che non dovranno più essere documentate nel DPS, tra cui:

- Nominare gli incaricati al trattamento dei dati personali (dipendenti o collaboratori);
- Nominare i responsabili esterni al trattamento di dati personali (ad es. consulenti del lavoro, commercialisti, avvocati, tecnici incaricati dell'assistenza sui sistemi informatici,…);
- Nominare gli Amministratori di Sistema e verificarne periodicamente l'operato;
- Attuare idonee misure di sicurezza per la protezione dei dati (controllo degli

accessi ai sistemi informatici, impiego di antimalware e firewall, effettuazione di backup dei dati informatici, ecc.);
- Rispettare le regole per la videosorveglianza;
- Verificare almeno annualmente la sussistenza dei profili di autenticazione;

Il nostro servizio consulenziale Vi consentirà di adeguare le Vostre procedure organizzative ed i Vostri Sistemi Informatici per poter affrontare con serenità gli adempimenti legislativi, senza temere le sanzioni previste.

La nostra proposta si articola nelle seguenti fasi:

- Check-up dell'organizzazione sulle procedure e sui sistemi informativi esistenti.
- Illustrazione delle azioni da intraprendere per essere conformi alla legge.
- Supporto alla Direzione per le decisioni da adottare e per l'applicazione delle azioni concordate.
- predisposizione/aggiornamento dei documenti relativi alla privacy..
- Formazione del personale.
- Verifica periodica dell'adeguatezza delle misure di sicurezza intraprese.

Per chi poi fosse interessato ad estendere le misure di sicurezza attuate per proteggere i dati personali e sensibili a tutti i dati aziendali, effettuando una valutazione più completa del rischio ed una gestione dello stesso in modo pianificato e documentato, potrebbe essere interessante valutare l'introduzione di un vero e proprio sistema di gestione per la sicurezza delle informazioni e certificarlo secondo la ISO 27001.

- Vademecum privacy e imprese
- Vademecum privacy e cloud computing

Alcuni link utili per maggiori informazioni sull'argomento:

- Scarica le Linee Guida del Garante della Privacy

- http://www.privacy.it/
- http://www.garanteprivacy.it/
- http://www.interlex.it/
- CloudWatch