



SUEDE.IT S.A.S

DEL DOTT. ALDO MAFFEI & C.

SERVIZI E TECNOLOGIE INFORMATICHE

Cdc Fsc / P IVA : 01709260507

VIA MARCO POLO, 11

56029 SANTA CROCE SULL'ARNO PI

T 057 132 132

Alla cortese attenzione del

Responsabile della Sicurezza dei dati personali

Santa Croce sull'Arno, 26 Febbraio 2009

Oggetto: Istruzioni importanti per la gestione della Privacy in azienda.

Riteniamo utile ricordarLe alcune regole da rispettare o far rispettare dalle persone coinvolte nella gestione della privacy:

- a) È opportuno che la Sua nomina sia riportata in un verbale del consiglio di amministrazione con data antecedente all'incarico affidatoLe. Se il responsabile è il titolare od il rappresentante legale il verbale non occorre.
- b) Entro il 31 marzo di ogni anno Vi sarà stampato il documento riepilogativo delle misure minime di sicurezza adottate secondo le Vs. informazioni ; dovete **firmarlo** e tenerlo a disposizione degli organi di vigilanza.
- c) La **password** è necessaria per la gestione elettronica dei dati aziendali ed è opportuno verificare periodicamente che le persone incaricate si attengano alle istruzioni ricevute, aprendo periodicamente la busta e provando la password davanti all'incaricato che subito dopo ne formulerà un'altra; la password deve essere cambiata ogni 6 mesi per il trattamento di dati comuni e/o ogni 3 mesi per quelli sensibili
- d) **Ogni nuova persona** che entra e tratta (legge,registra,fotocopia o cancella), i dati personali in maniera elettronica e/o cartacea **deve firmare** per accettazione la lettera di incarico contenente le regole a cui si deve attenere nel trattamento; se l'incaricato tratta i dati elettronici va attivata una password; quando l'incaricato si dimette o comunque non è più abilitato a trattare i dati in formato elettronico, deve essere disattivata la sua password.

Il personale deve essere istruito sulle modalità di gestione dei dati personali, siano essi in formato elettronico che cartaceo, con particolare riguardo ai dati sensibili ; gli incaricati devono firmare un documento ad uso interno che attesta la ricevuta istruzione.

Le lettere di incarico firmate devono esser conservate agli atti e se una persona si dimette, sopra la lettera di incarico va scritta la data di dimissione.

La stessa lettera di incarico deve essere fatta ai nuovi consulenti o terze parti che possono trattare i dati aziendali in Outsourcing.

Pag. 2

- e) Occorre fare particolare attenzione alla gestione dei **dati sensibili** che sono i dati personali che rivelano l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, adesione ai 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.

Quelli più facilmente presenti in azienda sono quelli in forma non elettronica, quali a semplice titolo di esempio: buste paga, curriculum vitae, il registro delle presenze del personale e degli infortuni, i certificati medici, le schede sanitarie, le informative di insolubilità clienti e gli insoluti in genere, le dichiarazioni dei redditi di tipo personale. Alla stregua dei dati sensibili sono quelli giudiziari, quali i certificati richiesti per l'espletamento di gare di appalto con enti pubblici.

Tutti questi documenti devono essere tenuti sotto chiave, non lasciati incustoditi sulla scrivania e trattati solo dalle persone incaricate.

I dipendenti devono firmare per accettazione la lettera informativa ex art.13 D .Lg . 196/03 che consente al datore di lavoro di fornire a terzi i loro dati sensibili per fini amministrativi , sanitari e fiscali.

La stessa informativa deve essere firmata da i consulenti che trattano per conto dell'azienda dati sensibili forniti dalla stessa per l'espletamento della loro attività.

Nel caso in cui i dipendenti siano autorizzati all' **uso di internet, il controllo sull' utilizzo deve essere regolamentato tramite un disciplinare interno**, diversamente l' eventuale controllo sull'uso di internet da parte del datore di lavoro può essere visto come violazione della loro privacy.

- f) Se avete il **sito WEB** con il quale consentite l'accesso a terzi per attività di informazione e/o attività commerciale, dovete inserire un'informativa specifica che preveda l'obbligo del consenso.

Vi ricordiamo che è obbligatoria l'esposizione della Vs. P.IVA sulla Home Page

Nel caso che le informazioni ricevute tramite internet Vi servano per creare una banca dati per utilizzo commerciale o profilazione dei nominativi ricevuti occorre fare la comunicazione preventiva al Garante di voler creare tale archivio e per quali scopi .

I ogni caso i dati personali raccolti NON possono essere ceduti a terzi senza espresso consenso dell'interessato

Chi svolge attività di **MARKETING** a mezzo INTERNET è tenuto ad acquisire il preventivo consenso da parte del destinatario, anche per e-mail .

- g) Il salvataggio dei dati dei server deve avere sempre cadenza giornaliera, con verifica dell'avvenuto salvataggio; è opportuno verificare periodicamente il ripristino degli stessi per accertarsi che i supporti siano validi.

E' consigliabile tenere un nastro di salvataggio per ogni giorno della settimana e se possibile in una stanza diversa da quella del server.

I supporti magnetici dismessi devono essere resi illeggibili smagnetizzandoli o distruggendoli.

Il salvataggio dei dati sulle singole postazioni P.C. (relativamente alla corrispondenza commerciale) deve avvenire almeno una volta la settimana.



SUEDE.IT S.A.S

DEL DOTT. ALDO MAFFEI & C.

SERVIZI E TECNOLOGIE INFORMATICHE

Cdc Fsc / P IVA : 01709260507

VIA MARCO POLO, 11

56029 SANTA CROCE SULL'ARNO PI

T 057 132 132

Pag. 3

Viene fornito per singola postazione un modulo sul quale rilevare le anomalie riscontrate che possono danneggiare i dati, quali virus e rottura del disco o dei supporti di salvataggio, annotando la soluzione adottata e le conseguenze del fatto.

E' opportuno riportare sul modulo anche l'eventuale uscita in riparazione e/o distruzione.

- h) Il collegamento ad Internet tramite **ADSL presuppone sempre l'installazione di un firewall** antintrusione ed è obbligatorio adottare l'antivirus su ogni postazione P.C. ed aggiornarlo più frequentemente possibile anche se il Personal non è abilitato all'uso di Internet
- i) Oltre al controllo sulla messa in sicurezza dei dati aziendali la Finanza può effettuare il controllo sull'esistenza della fattura di acquisto del software utilizzato. È bene quindi avere in una cartellina le fotocopie di tali documenti.
- j) In caso di controllo esterno e/o interno dell'azienda con **telecamera fissa**, con o senza supporto di registrazione magnetica, occorre sempre esporre sotto la stessa un cartello ben leggibile che ne segnala la presenza.

Nel caso in cui venga effettuata la registrazione deve essere nominato un incaricato alla revisione di quanto registrato.

I filmati registrati non devono contenere suoni, salvo casi in cui possa essere motivata da particolari esigenze di sicurezza.

Le registrazioni devono essere cancellate entro le 24h non festive successive alla registrazione

- k) Informateci tempestivamente se ricevete lettere di richiesta da persone od aziende sul trattamento dei loro dati personali in modo da rispondere nei termini di legge e non incorrere nel richiamo del Garante; tenete tutta la documentazione relativa alla privacy aggiornata e facilmente verificabile dagli organi di controllo

Vi ricordiamo che il mancato rispetto delle norme di sicurezza dei dati personali può comportare pesanti sanzioni pecuniarie e penali oltre al risarcimento dei danni alla parte lesa dal Vs. comportamento negligente.

Restiamo a Vs. disposizione per ulteriori chiarimenti.

SUEDE.IT Sas