TIVOLI JET srl

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

redatto ai. sensi e per gli effetti dell'articolo 34, comma l, lettera g) del dlgs 196/2003,
e del disciplinare tecnico allegato al medesimo decreto sub b)

Il presente documento intende assolvere all'obbligo dell'adozione di un *documento programmatico sulla sicurezza,* imposto dal punto 19 del disciplinare tecnico allegato B al Dlgs. 30.6.2003 n. 196 pubblicato nel S.O. 123 alla G.U. 174 del 29.07.2003 in presenza di dati sensibili o giudiziari.
Il documento è redatto per definire e descrivere le politiche di sicurezza adottate dalla Tivoli Jet srl ("società T.J.") in materia di trattamento di dati personali ed i criteri organizzativi seguiti per la loro attuazione.

Il presente documento è redatto e firmato in calce dal titolare del trattamento Maria Vallerignani.

1. L'elenco dei trattamenti dei dati personali gestiti

I dati trattati dal Titolare si possono suddividere come segue:
1 - Dati comuni relativi a clienti e fornitori
2 - Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali
3 - Dati di natura anche sensibile relativi a clienti

Strumenti utilizzati per il Trattamento

A - **Schedari ed altri supporti cartacei**
I supporti cartacei una volta terminato il ciclo lavorativo, vengono ordinatamente raccolti in appositi schedari situati in locali ad accesso selezionato e muniti di serratura.

B - **Elaboratori in rete privata**
Si dispone di una rete, realizzata mediante collegamenti interni via cavo, costituita da:
1. numero 1 server, localizzati nell'area ad accesso controllato degli uffici
2. numero 1 postazioni, dislocate in aree ad accesso controllato degli uffici
3. Tutte le postazione dispongono di collegamento ad Internet:

2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Le lettere di nomina dei responsabili e le lettere di incarico vengono raccolte in modo ordinato, in modo da fornire al titolare un quadro chiaro di chi fa cosa, nell'ambito del trattamento dei dati personali. Ogni anno si procede a verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

3. Analisi dei rischi che incombono sui dati

I rischi che incombono sui dati sono essenzialmente rappresentati da:

a)Calamità naturali:

1. Perdita di dati conseguente ad allagamento

2. Perdita di dati conseguente ad incendio

β)Minacce intenzionali

1) Accessi non consentiti:

a) Accesso, furto, manomissione di dati su supporti cartacei

b) Accesso,furto, manomissione di dati su supporti informatici

2)Accessi non autorizzati

3)Perdita di dati dovuta a virus o ad intrusione informatica

c)Minacce involontarie

l) Black out elettrico

2)Malfunzionamenti nel software

3)Malfunzionamenti hardware

4. Misure atte a garantire l'integrità e la disponibilità dei dati

a) Calamità naturali:

1. Perdita di dati conseguente ad allagamento:

Per ciò che concerne il rischio di perdita di dati da allegamento, considerata la posizione dell'ufficio sito in posizione sopraelevata rispetto al piano stradale si esclude che, salvo eventi imprevedibili e del tutto eccezionali, detto rischio possa verificarsi; ad ogni modo le attrezzature informatiche sono state tutte rialzate da terra,

2. Perdita di dati conseguente ad incendio:

Per ciò che concerne la perdita di dati conseguente ad incendio si precisa che sono state attuate tutte le misure previste dall'attuale legislazione in materia di prevenzione incendi, inclusa la verifica periodica di caldaie, impianto elettrico, impianto di riciclo d'aria e condizionamento; si precisa inoltre che la posizione di estintori risulta dalla planimetria affissa nei locali dello studio

b) Minacce intenzionali

1)Accessi non consentiti:

a) Accesso, furto, manomissione di dati su supporti cartacei

Si evidenzia che l'ingresso è protetto da una porta blindata mentre i restanti locali sono protetti da porte autonome per l'accesso.

Gli incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.

Le copie dei telefax inviati mediante apparecchio tradizionale vanno riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre quale primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax, con di seguito i fogli contenenti il messaggio.

Per ciò che concerne le trasmissioni del telefax, si raccomanda di inserire nella copertina del messaggio la presente dicitura:

"Qualora questo messaggio fosse da Voi ricevuto per errore vogliate cortesemente darcene notizia a mezzo telefax od e-mail e *distruggere il messaggio ricevuto erroneamente con il rimborso, da parte ns. dei costi da Voi sostenuti su Vostra esplicita richiesta. Quanto precede ai fini del rispetto del D.Lgs 196/03 sulla tutela dei dati personali. "*

La società T.J. è provvista di distruggi documenti: eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, ecc. vanno distrutte utilizzando detto apparecchio.

Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione.

Qualora i Sig.ri Clienti consegnino alla società documenti nelle mani degli incaricati questi dovranno essere raccolti in cartelline non trasparenti; qualsiasi documento che la società tramite gli incaricati al trattamento consegnano ai Sig.ri Clienti va inserito in apposite buste o cartelline non trasparenti:

I documenti giacenti sulle scrivanie, relativi a pratiche in corso, dovranno essere contenuti in cartelline non trasparenti; ogni qual volta l'incaricato si allontana dal posto di lavoro anche temporaneamente è chiamato a riporre i documenti nei cassetti con serratura in dotazione. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'incaricato debba continuare ad utilizzarli, nei giorni successivi.

I foglietti adesivi sui quali vengono annotati appunti vanno inseriti all'interno delle cartelline non trasparenti contenenti le pratiche.

Al termine del trattamento, l'incaricato dovrà invece restituire all'archivio gli atti e documenti non più necessari per lo svolgimento delle proprie mansioni lavorative.

Si procede ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudizi ari, dopo l'orario di chiusura tramite un apposito registro tenuto direttamente dal titolare del trattamento.

b. Accesso, furto, manomissione di dati su supporti informatici

La società T.J. ha attivato ed è correntemente funzionante un sistema d'autenticazione composta da un Username attribuito dal titolare e da una Password riservata conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente come riportato nel documento di nomina ad incaricato al trattamento.

2. Accessi non autorizzati

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni della struttura del Titolare.

3. Perdita di dati dovuta a virus od intrusione informatica

Virus

Per ciò che concerne la perdita di dati o di danneggiamento degli stessi dovuta a virus, si precisa che il server e i personal computers in dotazione allo studio sono dotati di programma antivirus "Symantec Norton Antivirus" che controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disc e cd rom.

L'aggiornamento alle nuove definizioni dei virus avviene automaticamente ogni settimana tramite una funzionalità a disposizione nel prodotto stesso.

Intrusione informatica

Relativamente all'intrusione informatica da parte di terzi, si precisa che è stato installato un firewall Software "Symantec Norton Internet Security" svolgente funzione di sistema di anti intrusione

c) Minacce involontarie

1. Black out elettrico

La società T.J.si è dotata di un gruppo di continuità per ogni elaboratore per prevenire le conseguenze dei blackout elettrici o dei picchi di sovra o sotto tensione elettrica.
Il gruppo di continuità in oggetto è in grado di filtrare l'alimentazione elettrica da eventuali impurità .

2. Malfunzionamenti nel software

A tale riguardo la società T.J. si avvale per ogni elaboratore del sistema operativo Windows Xp Professional che ha al suo interno una funzionalità che consente l'aggiornamento automatico delle "patch" rilasciate dalla casa madre volte a riparare i cosiddetti "bug" o errori di protezione del sistema operativo stesso. Agli incaricati viene data disposizione di installare tutte le patch che la Microsoft rilascia al fine di ridurre i rischi di malfunzionamenti del software.

3. Malfunzionamenti hardware

La manutenzione degli strumenti elettronici a livello hardware è stata affidata a ditte specializzate.

5. Criteri e modalità di ripristino dei dati, in seguito a distruzione o danneggiamento

Back up dati

Al fine di garantire non solo la integrità, ma anche la pronta disponibilità dei dati lo studio si è dotati di strumenti e procedure di backup che avvengono tramite una unità Imoega Zip.
Tutti i dati personali gestiti con strumenti elettronici nello studio vengono inclusi nella procedura di back up.
La frequenza con cui vengono effettuate le copie di sicurezza è settimanale. I supporti di back up vengono titolati e la loro custodia etichettata.
La società T.J. si è dotata di apposito armadio ignifugo e stagno per la conservazione e archiviazione dei supporti di salvataggio. E' fatto obbligo agli incaricati che procedono all'esecuzione del backup di conservare i supporti esclusivamente all'interno di questo armadio.
Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal punto 23 dell'allegato B del D.Lgs. 196/2003 in ipotesi di trattamento di dati sensibili.

6. Interventi formativi degli incaricati del trattamento

Sono stati organizzate all'interno della società T.J. e a cura del titolare due riunioni della durata di 2 ore ciascuna per informare i responsabili e gli incaricati del trattamento sulle nuove disposizioni del D.Lgs 196/03 in materia di tutela dei dati personali, elencando i rischi che incombono sui dati, le modalità per prevenire eventi dannosi e le misure di sicurezza adottate dal titolare. E' stato previsto che tali riunioni debbano essere ripetute ad ogni nuovo ingresso in

servizio di un dipendente, in occasioni di cambiamenti di mansioni, e in occasione della introduzione di nuovi significativi strumenti che modifichino le modalità di trattamento dei dati.

7. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati sensibili o giudiziari con strumenti elettronici vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si esige che il destinatario consegni una copia del documento programmatico sulla sicurezza redatto, o nel caso in cui il destinatario abbia affidato a soggetti esterni tali compiti consegni una copia del certificato di conformità rilasciato da chi ha curato la progettazione e l'attuazione delle misure minime di sicurezza.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

8. Dichiarazioni d'impegno e firma

Il presente documento, redatto il 30 dicembre 2004, viene firmato in calce da:

- Maria Vallerignani in qualità di rappresentante legale e in qualità di responsabile per la sicurezza.

L'originale del presente documento viene custodito presso la società T.J., per essere esibito in caso di controlli. Una sua copia verrà consegnata al responsabile del trattamento dei dati personali, ad ogni incaricato al trattamento dei dati personali e a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali come ad esempio, nel caso in cui dovessimo essere nominati responsabili per determinati trattamenti di dati personali.

Roma, 30 marzo 2009

Firma del responsabile ..... Firma del Titolare .....

TIVOLI JET s.r.l.
Via Colle Modello, 45
La Botte Guidonia (Rm)
Part.IVA 01826341008.
Cod. Fisc. 07631120586