Studio MARCHESICH NADIA

AGGIORNAMENTO DEL

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, 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 da **MARCHESICH NADIA** 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 MARCHESICH NADIA.

Indice

Nel rispetto del disciplinare tecnico di cui sopra si forniscono idonee informazioni riguardanti:

1. L'elenco dei trattamenti dei dati personali gestiti da MARCHESICH NADIA

I dati trattati dal Titolare si possono suddividere come segue:

- Dati comuni relativi a clienti
- Dati comuni relativi a fornitori
- Dati relativi allo svolgimento di attività economiche ed alle informazioni commerciali
- Dati relativi al personale, nonché ai candidati per diventarlo, di natura anche sensibile
- Dati di natura anche sensibile relativi a clienti

I dati relativi ai clienti sono trattati per le seguenti finalità:

contabilità
consulenza fiscale e societaria
dichiarazioni fiscali
gestione del personale

I dati relativi ai dipendenti sono trattati per le seguenti finalità:

gestione del personale

Strumenti utilizzati per il trattamento

A – Schedari ed altri supporti cartacei

I supporti cartacei, ivi inclusi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica cui si riferiscono, per essere archiviati una volta terminato il ciclo lavorativo, come segue:

- in archivio di pratiche di natura comune relative a clienti e fornitori, in particolare raccoglitori di cartelle con chiusura a chiave

C – Elaboratori in rete privata

Per elaboratori in rete privata si intendono quelli accessibili da altri elaboratori, o più in generale da altri strumenti elettronici, solo attraverso reti proprietarie, sulle quali possono viaggiare unicamente i dati del titolare del sistema.

Si dispone di una rete, realizzata mediante collegamenti interni via cavo, costituita da:

- numero 2 postazioni fisse, di cui 1 con accesso ad internet
- numero 2 stampanti
- altre periferiche: scanner, unità di copia removibili.

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

A – Responsabile del trattamento dei dati

Per il trattamento dei dati personali, il Titolare:

ha nominato responsabile il Titolare stesso.

B – Incaricati del trattamento dei dati

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante documentata preposizione di ogni persona ad una unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

● procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune,

● modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti,

● modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave,

● prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro mediante:

● disconnessione utente

● procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi

● procedure per il salvataggio dei dati

● modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali

● dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all' organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (***mansionario privacy***), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

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

b) 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

1. Black out elettrico
2. Malfunzionamenti nel software
3. Malfunzionamenti hardware

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

Calamità naturali:

1. Perdita di dati conseguente ad allagamento:

Per ciò che concerne il rischio di perdita di dati da allagamento, considerata la posizione del fabbricato dello Studio 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 in duplice copia nei locali dello Studio richiamando inoltre le norme di comportamento da seguire in caso di incendio, anch'esse affisse nei locali.

Minacce intenzionali

1. Accessi non consentiti:

a) Accesso, furto, manomissione

Si evidenzia che:
lo Studio è protetto da:
● Gli ingressi dello Studio sono protetti da porte blindate
I locali nei quali si svolge il trattamento sono inoltre protetti da:
● chiusura a chiave delle porte di accesso alle stanze contenenti i dati.

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.
Eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, ecc. vengono distrutti al termine del loro utilizzo.
E' fatto espresso divieto di utilizzare carta riciclata per stampare documenti da consegnare a terzi. L'utilizzo è consentito esclusivamente per uso interno al fine di limitare la possibilità di fornire erroneamente informazioni a persone non autorizzate.

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. A tale fine, gli incaricati sono stati dotati di:

● cassetti con serratura
● armadi chiudibili a chiave
● cassaforte

nei quali devono riporre i documenti, contenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. 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.

Al termine del trattamento, l'incaricato dovrà invece riporre in archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.

Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree, nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali, in modo distinto per le diverse funzioni aziendali.

Particolari cautele sono previste per l'archiviazione di documenti, atti e supporti contenenti dati sensibili o giudiziari: essa deve avvenire in luoghi, armadi, casseforti, o dispositivi equipollenti, che possano essere chiusi a chiave.
Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti:

● le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'incaricato che ha il compito di custodirla

Si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, mediante l'adozione dei seguenti accorgimenti :

● la chiave dell'archivio è affidata, dopo l' orario di chiusura, al titolare o ai responsabili del trattamento, o in alternativa ad uno o più soggetti incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di cloro che hanno richiesto di accedere all' archivio

● l'accesso ai dati avviene esclusivamente da parte del titolare dello Studio.

Gli impianti ed i sistemi di cui è dotata l' organizzazione appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti. Per l'anno 2005 sono quindi previsti semplicemente interventi di manutenzione.

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

lo Studio ha attivato, ed è correntemente funzionante, un sistema d' autenticazione per ognuno degli incaricati che trattano dati personali:

● si associa un codice per l'identificazione dell'incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente

Per l'attribuzione e la gestione delle credenziali per l' autenticazione si utilizzano i seguenti criteri:

● ad ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Il codice per l'identificazione (username), attribuito all' incaricato da chi amministra il sistema, è univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.

Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti nell'elaborazione delle password:

- esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino),
- buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica.

La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).

Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.

Nell' ipotesi di trattamento di dati sensibili viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 3 mesi.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento
- in ogni caso, entro sei mesi di mancato utilizzo.

Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili che possono gestire e contenere dati personali.

Per quanto concerne i supporti rimovibili (es. floppy disk, chiavette hard disk, cd riscrivibili ZIP,…), contenenti dati personali, la norma impone particolari cautele solo nell' ipotesi in cui essi contengano dati sensibili o giudiziari.
La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi,

una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

2. Accessi non autorizzati

Per quanto concerne il rischio di accessi non autorizzati, non appare necessario prevedere profili di autorizzazione distinti, per le diverse persone, in relazione alle limitate dimensioni della struttura del Titolare ed al fatto che non si ravvisano ragioni di tutela della riservatezza tali, da imporre che uno o più incaricati non possano accedere ad alcune tipologie di dati personali oggetto di trattamento.

3. Perdita di dati dovuta a virus od intrusione informatica

a) Virus

Per ciò che concerne la perdita di dati o di danneggiamento degli stessi dovuta a virus, si precisa che:

● i personal computers in dotazione allo Studio sono dotati di programma antivirus NORTON ANTIVIRUS 2004 prodotto dalla ditta SYMANTEC

L' antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disk e cd rom.

Il personale è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici nello Studio.

L'aggiornamento alle nuove definizioni dei virus avviene, per i personal computers, automaticamente ogni giorno tramite una funzionalità a disposizione nel prodotto stesso.

b) Intrusione informatica

Relativamente all'intrusione informatica da parte di terzi, si precisa che è stato installato un firewall hardware. Il firewall è stato configurato dalla società S.M.A. S.R.L. specializzata in sicurezza informatica che ha fornito anche direttive e indicazioni in merito alla sua manutenzione periodica.

Anche in relazione a questo rischio non si registrano inconvenienti occorsi, sicché si reputa il sistema di protezione rispondente alle necessità dello Studio.

Minacce involontarie

Malfunzionamenti nel software

A tale riguardo la nostra organizzazione si doterà di tali programmi entro il 31 marzo 2006. Successivamente, l'aggiornamento di tali programmi avverrà con cadenza almeno annuale, che diviene semestrale per gli strumenti con i quali si trattano dati sensibili o giudiziari.

Malfunzionamenti hardware

In relazione a questo rischio lo Studio non ha affidato la manutenzione degli strumenti elettronici ad una specifica ditta ma ha ritenuto di avvalersi di volta in volta dell'operatore del settore che garantisca l'intervento più celere possibile al fine di ridurre al minimo i tempi di ripristino del corretto funzionamento dello strumento elettronico.

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 dotata dei seguenti strumenti e procedure di back up:

- masterizzatore cd
- disco rigido removibile; chiave usb; copia su pc in altra partizione del disco rigido.

Tutti i dati personali gestiti con strumenti elettronici nello Studio vengono inclusi nella procedura di backup.

La frequenza con cui vengono effettuate le copie di sicurezza è settimanale, solitamente il venerdì.
I supporti di back up vengono titolati e la loro custodia etichettata.

Le ultime copie di backup vengono riposte in un locale dello Studio in una cassaforte.

Le penultime copie di backup dati vengono tenute in locali diversi dallo Studio e precisamente in abitazione del titolare dello studio.

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.

Il ripristino avviene mediante apposito programma di restore in dotazione all'unità preposta al backup.
L'addetto al Disaster Recovery nonché custode dei supporti di backup è il titolare dello Studio.

6. Interventi formativi degli incaricati del trattamento

lo Studio riconosce l'importanza della formazione dei suoi componenti riguardo le tematiche della sicurezza, come elemento significativo di riduzione dei rischi al proprio sistema informativo e s' impegna a promuovere momenti formativi in particolare al momento dell'ingresso in servizio o al momento di cambiamenti di mansioni di tali soggetti o all' introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.

Tutti i componenti dello Studio devono comunque partecipare una volta all'anno ad un corso di approfondimento e mantenimento delle conoscenze, finalizzato a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi
- modalità per aggiornarsi sulle misure di sicurezza.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali

in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi per l'anno in corso sono stati così programmati:

- data 03/12/2005 durata 1 ore a cura del titolare dello Studio

7. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all' esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell' ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

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 30/11/2005, viene firmato in calce da:

● MARCHESICH NADIA, in qualità di titolare dello Studio;

L' originale del presente documento viene custodito presso la sede dello Studio, per essere esibito in caso di controlli.

Una sua copia verrà consegnata:

● a chiunque ne faccia richiesta, in relazione all' instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali

TRIESTE, 30/11/2005.

Firma del rappresentante
legale dello Studio