

MEMORANDUM IN MATERIA DI SICUREZZA NEL TRATTAMENTO DI DATI PERSONALI

A tutti gli incaricati del
Trattamento di dati personali
-- sede --

Premesse:

Il Dlgs. 196/2003 (anche noto come Codice sulla Privacy) è entrato in vigore il 1.1.2004. Raccoglie in un Testo Unico le precedenti Leggi, Decreti e Codici Deontologici in tema di Privacy. Le Aziende che trattino dati personali, di fatto tutte le Aziende, devono trattare tali dati in conformità al Codice stesso.

Per essere conformi, le aziende devono agire su tre fronti:

1. pianificare misure organizzative, amministrative e tecniche di sicurezza attraverso un documento formale conosciuto come Documento Programmatico sulla Sicurezza;
2. adeguarsi alle misure tecniche minime di sicurezza definite nell'allegato B del Dlgs. 196/2003;
3. dare informativa trasparente e completa (se e quando dovuta) dei trattamenti dei dati personali ai relativi interessati ed ottenerne il consenso (se e quando necessario).

Trattare dati personali in non-conformità con la Legge, espone l'azienda sul piano **civile** e **penale** con sanzioni **amministrative** fino a 90.000 Euro (fatti comunque salvi i risarcimenti eventualmente dovuti in sede civile) e può esporre i suoi dipendenti ed il suo Legale Rappresentante a sanzioni penali fino a **tre** anni di detenzione.

Il primo e più significativo passo verso la conformità è la stesura del "Documento Programmatico sulla Sicurezza" -- un documento che descrive i trattamenti di dati personali trattati in Azienda, l'organizzazione di sicurezza dell'Azienda e analizza i rischi che incombono sui dati personali. Si tratta di un'analisi strutturata dei dati personali trattati in Azienda, dell'organizzazione della sicurezza dei dati e delle misure in essere e da pianificare per mettere e mantenere in sicurezza i dati. Da questo documento derivano tutte le altre azioni richieste dal Dlgs.196/2003: misure minime, informative, lettere d'incarico al personale preposto ai trattamenti.

I dati personali sono quelli che identificano una persona FISICA o GIURIDICA. Pertanto tutte le Aziende trattano dati personali, anche solo per il fatto di gestire un archivio cartaceo od informatico dei Clienti/utenti o altri archivi che contengano i dati identificativi di persone o aziende (fascicoli del personale, elenco negozi, albo delle associazioni, ruoli tributari ...).

I dati personali sensibili sono quelli che indicano o "sono idonei" a rilevare, fra gli altri, dati personali quali le idee religiose, politiche e filosofiche, lo stato di salute o la vita sessuale, l'origine razziale ed etnica. La questione non è ovvia. Solo un'analisi attenta dei trattamenti effettuati in Comune può rilevare se trattiamo o meno "dati sensibili", che dovranno essere trattati con maggiore cautela rispetto ai dati personali non sensibili. Infatti, anche dati apparentemente innocui possono rivelarsi "idonei" a fornire dati personali sensibili. Per esempio: la foto degli stranieri sul permesso di soggiorno (quando non sia già sufficiente il nome !), permette di capire l'origine razziale.

La sicurezza:

Nodo centrale del nuovo Codice è l'attenzione da porre all'aspetto della sicurezza dei dati. A tal fine ricordo che con atto prot. n. 2811 del 29.3.2004 i Sigg. Crippa Gianfranco e Targonato Silvia sono stati nominati amministratori di sistema. La loro responsabilità in materia di sicurezza è limitata alle banche dati informatiche sui server.

I responsabili del trattamento (coincidenti con i responsabili di area e di procedimento) sono responsabili anche del profilo della sicurezza, per tutti i trattamenti eseguiti dagli incaricati del proprio ambito di responsabilità.

Gli incaricati non sono comunque esentati dall'applicare puntualmente e correttamente alcune cautele, che vengono di seguito specificate.

Istruzioni:

Tanto premesso, si forniscono agli incaricati ed ai responsabili del trattamento le seguenti istruzioni per applicare le norme di sicurezza meglio dettagliate nel Documento Programmatico approvato con deliberazione della Giunta Comunale n.... del

ANALISI DEI RISCHI:

Le banche dati in cui sono conservati i dati personali, siano esse in forma cartacea che archivi informatizzati (sul server o localmente sui client), sono soggette a rischi di perdita e danneggiamento.

Il documento programmatico della sicurezza riporta un'analisi accurata dei rischi che incombono sui dati e delle misure esistenti o in previsione per prevenire eventi dannosi.

Conoscere i rischi aiuta a comprendere la collaborazione richiesta agli incaricati del trattamento: si invita a voler prendere visione del suddetto Documento Programmatico.

SICUREZZA DEL SOFTWARE:

- Presso ciascun ufficio è consentita l'installazione esclusiva delle seguenti categorie di software:
 - a) Software commerciale dotato di licenza d'uso (esempio: pacchetti di office automation)
 - b) Software gestionale realizzato specificatamente per l'Amministrazione Comunale dalle ditte specializzate nel settore della P.A. (es: applicativi in uso al personale)
 - c) Software gestionale realizzato specificatamente dagli organi centrali della Pubblica Amministrazione (es. Istat, INPS, Ministeri ..)
- L'eventuale installazione di software diversi deve essere preventivamente valutata e autorizzata dai responsabili della sicurezza.
- Al fine di prevenire ed evitare la diffusione di virus informatici, il software viene installato solo da supporti fisici originali dei quali è ben nota la provenienza.

SALVATAGGIO DEI DATI (BACKUP):

- In casi particolari, il backup viene effettuato localmente nell'ambito di taluni uffici. In questo caso l'incaricato effettua le seguenti operazioni:
 - Esecuzione quotidiana del backup, eventualmente tramite procedure automatiche
 - Copia del risultato di backup sul server allo scopo di consentirne il salvataggio quotidiano con le modalità di cui ai punti precedenti.
- Ulteriori accorgimenti a tutela del trattamento di dati sensibili, consentono:
 - Il salvataggio temporaneo automatico con periodicità inferiore a 10 minuti
 - Il salvataggio eventuale su hard disk del PC con registrazione protetta da password scelta dall'utente
 - Compressione dei dati elaborati in appositi file di tipo "zip" per eventuale invio all'indirizzo e-mail noto e certo (certificato)

PROTEZIONE ANTIVIRUS:

- Tutti gli elaboratori ed i server di rete sono protetti contro il rischio di intrusione mediante apposito software antivirus (Norton Antivirus). Due volte al giorno viene effettuato l'aggiornamento automatico programmato del software antivirus con connessione automatica via internet al sito del produttore (Symantec).
- In mancanza di procedure di installazione automatiche, gli incaricati del trattamento sono stati istruiti per effettuare l'aggiornamento del software antivirus sulle postazioni di lavoro di propria competenza, con cadenza settimanale.

PASSWORD:

- Una prima password viene richiesta all'utente al momento dell'accensione del PC, limitando di fatto l'accesso immediato alla macchina ("*password del BIOS*");
- Una volta avuto accesso alla macchina, viene richiesto l'inserimento del nome utente e di un'ulteriore password (diversa dalla precedente). Il nome utente è preconfigurato per delimitare l'ambito di accesso dell'utente così connesso ai diversi ambienti della rete aziendale (dalla posta elettronica all'accesso a cartelle condivise);
- La password del BIOS e quella di accesso alla rete:
 - Non devono derivare dal nome utente o dai dati personali dell'utente né contenere riferimenti agevolmente riconducibili all'incaricato;
 - Devono avere lunghezza minima di otto caratteri oppure, qualora lo strumento non lo permetta, da un numero di caratteri pari al massimo consentito;
 - Sono strettamente personali: l'utente è tenuto a non comunicarle a terzi ed a non annotarle in vicinanza della propria postazione di lavoro o comunque in luoghi incustoditi;
- Le password in uso vengono modificate dai responsabili della sicurezza con cadenza trimestrale, comunicate agli incaricati e da questi ultimi modificate al primo utilizzo.

COPIE DELLE CREDENZIALI:

- La custodia delle copie delle credenziali si rende necessaria per assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

INDIVIDUAZIONE DEI RISCHI:

- Gli amministratori di sistema provvedono ad informare tempestivamente i responsabili del trattamento dati di ogni eventuale problema di sicurezza di cui dovessero venire a conoscenza;
- I soggetti responsabili del trattamento provvederanno di conseguenza, anche per tramite degli amministratori di sistema, a informare tempestivamente gli incaricati:
 - della presenza di virus negli elaboratori dell'ufficio;
 - di prassi da parte del personale non conformi alle disposizioni di sicurezza;
 - della periodica necessità di variazione delle parole chiave da parte degli incaricati;
 - della disponibilità di programmi di aggiornamento relativi all'antivirus;
 - della perdita delle qualità che consentono all'incaricato l'accesso ai dati personali
- I responsabili, in caso di necessità, provvederanno ad organizzare iniziative per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.