



## DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI

Oltrona San Mamette, 13 Marzo 2006

Il sottoscritto **Carlo Galimberti**, legale rappresentante di **MTA GROUP Srl**, titolare del trattamento di dati personali disciplinato dal D. Lgs. 30.6.2003, n.196 – Codice in materia di protezione dei dati personali – a norma degli artt. 33/36 e del disciplinare tecnico (Allegato B) relativi al trattamento dei dati personali non sensibili e giudiziari effettuato manualmente e/o con strumenti elettronici, adotta il seguente documento programmatico.

### ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Le attività di trattamento consistono in:

- raccolta
- registrazione
- organizzazione
- conservazione
- consultazione
- elaborazione
- modificazione
- selezione
- estrazione
- raffronto
- utilizzo
- interconnessione
- blocco
- comunicazione
- diffusione
- cancellazione
- distruzione

*di dati personali non sensibili/giudiziari quali*

- Informazioni concernenti taluni procedimenti giudiziari;
- Codice fiscale ed altri numeri di identificazione personale (carte sanitarie);
- Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica, posizione rispetto agli obblighi militari, numero carta di identità, passaporto, patente di guida, numero di posizione previdenziale o assistenziale, targa automobilistica, dati fisici, altezza, peso, ecc.);

---

#### MTA Group srl

Mechanical Technology Applied  
22070 OLTRONA SAN MAMETTE - COMO  
Via Giamminola, 14 - tel. 031.891.766 - Fax 031.934.793 -  
Email: mtagroup@mtagroup.it - Web: www.mtagroup.it



- Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare);
- Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente (benefit e altro), dati sulla gestione e sulla valutazione delle attività lavorative, cariche pubbliche rivestite);
- Attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, redditi, beni patrimoniali, investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali);
- Istruzione e cultura (curriculum di studi e accademico, pubblicazioni - articoli, monografie, relazioni, materiale audio-visivo, ecc... - titoli di studio);
- Dati sul comportamento (profili personalità/caratteriali);
- Abitudini di vita e consumo;

*Organizzati nelle seguenti banche dati*

- Archivio dati clienti
- Archivio dati fornitori
- Archivio lavori
- Archivio dati dipendenti / collaboratori / titolari

**LUOGHI DI TRATTAMENTO**

- Sede di Via Giamminola, 14 - 22070 OLTRONA SAN MAMETTE - Como

**DISTRIBUZIONE DI COMPITI E RESPONSABILITA' NELLE STRUTTURE CHE TRATTANO DATI PERSONALI**

*DIREZIONE GENERALE*

I membri della Direzione Generale hanno accesso a tutti i livelli delle banche dati. Strumenti elettronici utilizzati: dispongono di un elaboratore collegato alla rete aziendale e con accesso totale alle cartelle di archiviazione ed al software gestionale dell'azienda.

*RESPONSABILE SERVIZIO VENDITE*

Il Responsabile del Servizio Vendite ha accesso a tutti i livelli delle banche dati. Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed al software gestionale aziendale.



#### *RESPONSABILE SERVIZIO APPROVVIGIONAMENTI*

Il Responsabile del Servizio Approvvigionamenti ha accesso a tutti i livelli delle banche dati.

Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed al software gestionale aziendale.

#### *RESPONSABILE SERVIZIO TECNICO*

Il Responsabile del Servizio Tecnico ha accesso a tutti i livelli delle banche dati.

Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed agli strumenti di disegno tecnico.

#### *ADDETTO SERVIZIO TECNICO*

Gli addetti al Servizio Tecnico hanno accesso a tutti i livelli delle banche dati.

Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed agli strumenti di disegno tecnico.

#### *RESPONSABILE SERVIZIO AMMINISTRATIVO E DEL PERSONALE*

Il responsabile del Servizio Amministrativo e del Personale ha accesso a tutti i livelli delle banche dati.

Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed al software gestionale aziendale.

#### *ADDETTO AL SERVIZIO AMMINISTRATIVO E DEL PERSONALE*

Gli addetti al Servizio Amministrativo e del Personale ha accesso a tutti i livelli delle banche dati.

Strumenti elettronici utilizzati: dispone di una postazione collegata alla rete aziendale e con accesso totale alle cartelle di archiviazione ed al software gestionale aziendale.

#### *COLLABORATORI COMMERCIALI*

I collaboratori commerciali non hanno accesso alle banche dati.

Strumenti elettronici utilizzati: hanno la possibilità di collegarsi alla rete aziendale per sfruttare la connessione internet ma con accesso controllato alle cartelle di archiviazione.

#### *AMMINISTRATORE DI SISTEMA E CUSTODE DELLE COPIE DELLE CREDENZIALI*

Ha accesso a tutti i livelli delle banche dati. Si occupa della realizzazione dei backup, degli aggiornamenti software, degli strumenti dedicati alla prevenzione. Controlla l'aggiornamento delle password custodendone una copia.



## ANALISI DEI RISCHI

Le violazioni alla sicurezza informatica previste sono molteplici, di provenienza interna o esterna<sup>1</sup> all'azienda, considerate con riferimento alla natura dei dati trattati, e raggruppabili in tre tipologie di "attacco".

### ATTACCHI FISICI

- Calamità naturali (inondazioni, terremoti, fulmini);
- Interruzione di servizi (energia elettrica, condizionamento, etc.);
- Accesso fisico ai locali non autorizzato (forzate finestre/porte);
- Danneggiamento accidentale d'origine umana (al sistema, ai terminali, alle apparecchiature, alle linee e ai cavi, etc.);
- Danneggiamento intenzionale d'origine umana (al sistema, ai terminali, alle apparecchiature, alle linee e ai cavi, etc.);
- Furto/duplicazione/lettura di supporti cartacei (es.: tabulati, disegni e documenti, carte di identificazione);

### ATTACCHI LOGICI

- Accessi non autorizzati ad elaboratori/apparati di rete, ai servizi di rete, agli applicativi e alle funzioni;
- Accesso e lettura non autorizzati di dati presenti su archivi informatici;
- Modifica non autorizzata di dati o di programmi;
- Inserimento non autorizzato di software;
- Alterazione dei dati di configurazione del sistema;
- Intercettazione delle informazioni;
- Lettura non autorizzata di schermate video;
- Furto/duplicazione/lettura di supporti magnetici (Cd-Rom, dischetti, token, smart-card);
- Malfunzionamento hardware e software;
- Analisi delle tipologie di traffico sulle linee di trasmissione dei dati (traffic analysis);
- Estrazione non autorizzata di informazioni/dati trasportati in Rete (sniffing)<sup>2</sup>;
- Lettura non autorizzata di dati di Rete (utilizzo non aziendale di Internet);
- Modifica non autorizzata di dati in fase di trasmissione;
- Replica di messaggi;
- Dirottamento dei risultati di una elaborazione;
- Mascheramento dell'originatore/destinatario, utente o sistema (spoofing);
- Decifratura di password (password cracking);

---

<sup>1</sup> Esempi di attacchi interni (es.: da parte di incaricati/addetti alle pulizie): distruzione di hardware e impianti; accessi non autorizzati ai dati/applicazioni; cancellazione/modifica di dati; pirateria/frode informatica; uso non aziendale della strumentazione. Fonti di attacchi esterni: aziende concorrenti; criminalità organizzata; terrorismo; hacker.

<sup>2</sup> Consiste nell'attività di installazione di programma su reti di computer fatta da un hacker al fine di raccogliere informazioni dai pacchetti che attraversano la Rete e che gli vengono poi inoltrate. La potenziale installazione di programmi sniffer (che servono anche ad intercettare password e nomi utente da utilizzare in un attacco successivo) è una delle principali ragioni per la quale gli utenti non devono installare software non testato sui propri computer.



## ATTACCHI ORGANIZZATIVI

Si identificano nella gestione inadeguata della sicurezza per carenze relative a:

- Rilevazione e valutazione dei rischi ;
- Aggiornamento dell'analisi;
- Misure protettive ed aggiornamenti tecnologici necessari;
- Cultura ed informazione aziendale sulla sicurezza;
- Assegnazione ed istruzioni agli incaricati;
- Classificazione dei dati;
- Registrazione delle consultazioni;
- Documentazione dei controlli periodici;
- Verifiche periodiche su dati/trattamenti non consentiti/corretti;
- Distruzione controllata dei supporti;
- Piano di disaster recovery;

## MISURE ADOTTATE/DA ADOTTARE

Sulla scorta dell'analisi dei rischi, oltre a quelle in ottemperanza alle disposizioni del disciplinare tecnico, sono adottate/da adottare le seguenti misure:

### - PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

Contro

- errori accidentali → (adeguata formazione ed istruzioni agli incaricati; standardizzazione e chiarezza delle informazioni da dare agli incaricati; raccolta presso gli incaricati dei dati relativi all'evento ai fini di prevenzione)
- errori di programmazione → (test e verifiche)
- vulnerabilità del sistema operativo (bugs) → (patch mensili?)
- accessi abusivi ed intrusioni → (divieto di installare programmi non testati)
- attacchi da virus, worm, malware<sup>3</sup>, etc. → (antivirus quotidiani, divieto di installare software non testato)
- violazione riservatezza ed integrità dei messaggi → (autorizzazioni)

### - PER LA PROTEZIONE DI AREE E LOCALI

- Vigilanza della sede;
- Sistemi di allarme;
- Ingresso controllato ai locali di trattamento;
- Autenticazione degli accessi;
- Custodia in armadi/classificatori non accessibili;
- Custodia in armadi blindati e/o ignifughi;
- Deposito in cassaforte;
- Custodia dei supporti in contenitori sigillati;

---

<sup>3</sup> I MalWare: sono virus e worm che hanno per finalità la raccolta di informazioni all'interno di una intranet aziendale.

- Continuità dell'alimentazione elettrica e del condizionamento;
- Dispositivi antincendio;
- Controllo sull'operato dei manutentori;

### **PER IL TEMPESTIVO RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN CASO DI DANNEGGIAMENTO DEGLI STESSI O DEGLI STRUMENTI ELETTRONICI**

#### **• Criteri e modalità del ripristino**

Quotidianamente un software dedicato realizza la copia di tutti gli archivi informatici su un hard-disk esterno.

Test di ripristino parziale vengono effettuati settimanalmente.

#### **• Soggetti incaricati al controllo del funzionamento delle copie**

Il controllo dei back-up viene effettuato dall'incaricato all'amministrazione del sistema.

#### **• Luoghi di custodia**

L'incaricato all'amministrazione del sistema trasporta quotidianamente presso il proprio domicilio le copie di back-up realizzate.

#### **NOTA**

Sulla scorta delle copie controllate si provvede al ripristino, consistente:

- in una nuova installazione di tutti i file di dati e programmi che l'evento indesiderato ha alterato o distrutto;
- oppure nella sostituzione delle componenti tecnologiche hardware che hanno provocato l'interruzione.

Se l'evento è accaduto a causa di una vulnerabilità del sistema (bugs) si provvederà ad installare anche la patch correttiva della vulnerabilità individuata.

### **PER LA FORMAZIONE DEGLI INCARICATI**

Si prevedono interventi formativi al momento dell'ingresso in servizio e in occasione di

- cambiamento di mansioni;
- introduzione di nuovi strumenti rilevanti per il trattamento;
- emanazione di norme integrative modificative rilevanti in materia di privacy

Gli interventi formativi dovranno mirare a rendere edotti gli incaricati:

- dei rischi che incombono sui dati;
- delle misure disponibili per prevenire eventi dannosi;
- delle norme sulla protezione dei dati più rilevanti nelle attività di competenza;
- delle responsabilità che ne derivano;
- dei modi di aggiornarsi sulle misure adottate dal titolare.

**PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME IN CASO DI TRATTAMENTO AFFIDATO ALL'ESTERNO DELLA STRUTTURA**

- Affidamento solo a società di servizi che, per esperienza, capacità ed affidabilità, fornisca idonea garanzia del pieno rispetto delle norme sulla sicurezza;
- Dettagliata esposizione contrattuale delle "misure di sicurezza" da adottare e delle relative responsabilità civili e penali;
- Obbligo di rendere noti gli eventuali attacchi e le contromisure effettuate;
- Verifiche<sup>4</sup> nella gestione della sicurezza;
- Ispezioni<sup>5</sup> con regolarità;

Il Legale Rappresentante

---

---

<sup>4</sup> Sull'andamento a lungo termine.

<sup>5</sup> Possono essere non calendarizzate.