

O.M.T.R. SRL

Via Del Piano Grande 10/B
- 21050 CANTELLO (VA)
Cod.Fisc. e P.Iva 02847440126 – R.E.A. Varese n. 294829
Reg. Imp. Varese -Cap.soc. Euro 50.000
Tel. 0332/ 417141 - fax. 0332/418521

Sede Operativa:
Via Vespucci, 2
26010 Ripalta Cremasca (CR)

Tel.0373/268927 – fax 0373/680921

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)**

AGGIORNAMENTO DEL 30 MARZO 2009

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 **O.M.T.R. SRL** 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 O.M.T.R. SRL in persona del suo legale rappresentante CARAVATI GIAMPIERO.

Indice

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

1.	punto 19.1 del disciplinare: <i>l'elenco dei trattamenti di dati personali gestiti nell'Azienda</i>
2.	punto 19.2 del disciplinare: <i>distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati</i>
3	punto 19.3 del disciplinare: <i>l'analisi dei rischi che incombono sui dati</i>
4	punto 19.4 del disciplinare: <i>le misure di sicurezza adottate e da adottare, per garantire l'integrità e la disponibilità dei dati, protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità</i>
5	punto 19.5 del disciplinare: <i>i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento</i>
6	punto 19.6 del disciplinare: <i>interventi formativi degli incaricati del trattamento</i>
7	punto 19.7 del disciplinare: <i>i criteri da adottare, per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno all'esterno della struttura del titolare.</i>
8	dichiarazioni d'impegno e firma

1. L'elenco dei trattamenti dei dati personali gestiti da O.M.T.R. SRL

I dati trattati dal Titolare si possono suddividere come segue:

- Dati comuni relativi a clienti.
- Dati comuni relativi a fornitori
- Dati (inclusi suoni ed immagini) idonei a rilevare la posizione di persone ed oggetti
- 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 idonei a rivelare lo stato di salute e/o la vita sessuale di collaboratori

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:

- archivio di pratiche di natura comune relative a clienti e fornitori
- archivio di pratiche di natura sensibile relative ai dipendenti

B – Elaboratori non in rete

Per elaboratori non in rete si intendono quelli non accessibili da altri elaboratori, terminali o, più in generale, da altri strumenti elettronici.

Essi sono costituiti da:

- numero 2 stampanti

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 5 postazioni fisse, di cui 5 con accesso ad internet
- numero 2 stampanti
- numero 1 altri strumenti elettronici (scanner,..)

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

Per il trattamento dei dati personali, il Titolare non ha nominato responsabili.

- L'Amministratore di sistema è il signor Caravati Giampiero.

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.

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:
 - 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 rimovibili, 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.

Azienda O.M.T.R. SRL

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.

Sono previsti **interventi formativi degli incaricati del trattamento**, finalizzati 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, adottate dal titolare.

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 implicino modifiche rilevanti rispetto al trattamento di dati personali
- in occasione della introduzione di nuovi significativi strumenti, che implicino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

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 Azienda 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 Azienda 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 di dati su supporti cartacei

Si evidenzia che:

- I locali nei quali si svolge il trattamento sono protetti da sistemi di allarme
- 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.

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 ed armadi chiusi a chiave, nei quali devono riporre i documenti, contenuti 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.

Azienda O.M.T.R. SRL

Al termine del trattamento, l'incaricato dovrà invece restituire all'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 possono essere chiusi.

Dopo l'orario di chiusura nessuno è autorizzato ad accedere a dati personali se non i titolari dell'attività.

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 2009 sono quindi previsti semplicemente interventi di manutenzione.

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

l'Azienda 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:

Azienda O.M.T.R. SRL

- 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). Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli incaricati sono state fornite istruzioni scritte, affinché essi:

- scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata
- consegnino la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

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 e sui palmari che possono gestire e contenere dati personali .

Per quanto concerne i supporti rimovibili (es. floppy disk, chiavette hard disk, cd riscrivibili, etc), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili o giudiziari.

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 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 computer in dotazione all'Azienda sono dotati di programma antivirus SIMANTEK che garantisce annualmente l'aggiornamento.

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 nell'Azienda.

L'aggiornamento alle nuove definizioni dei virus avviene automaticamente ogni giorno tramite una funzionalità integrata 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 SIEL.CO. SRL 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 dell'Azienda.

Minacce involontarie

Black out elettrico

L'Azienda si è dotata dei seguenti gruppi di continuità per prevenire le conseguenze dei blackout elettrici o dei picchi di sovra o sotto tensione elettrica.:

- n. 3 A P C.

I gruppi di continuità in oggetto sono in grado di filtrare l'alimentazione elettrica da eventuali impurità.

Malfunzionamenti nel software

A tale riguardo la nostra organizzazione si è da tempo dotata di tali programmi, per la protezione da malfunzionamenti degli strumenti elettronici, che provvede ad aggiornare con cadenza almeno annuale, che diviene semestrale per gli strumenti con i quali si trattano dati sensibili o giudiziari.

Malfunzionamenti hardware

La manutenzione degli strumenti elettronici sia a livello hardware sia a livello software viene affidata alla ditta SI.EL.CO. SRL.

Quando è necessario si provvede alla sostituzione del macchinario più datato.

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 l'Azienda si è dotata dei seguenti strumenti e procedure di back up:

- unità nastro

Tutti i dati personali gestiti con strumenti elettronici nell'Azienda vengono inclusi nella procedura di backup gestita dal software Symantec Backup Exec ed effettuati dalla ditta EPOX SRL tramite SERVER in rete.

La frequenza con cui vengono effettuate le copie di sicurezza è giornaliera per 5 giorni alla settimana; successivamente si procede alla sovrascrittura di quelle della settimana precedente; le copie di ogni lunedì vengono conservate per 5 settimane prima della sovrascrittura.

I supporti di back-up vengono titolati e la loro custodia etichettata.

Le ultime copie di backup vengono riposte in una cassetta ignifuga presso un locale dell'Azienda (sempre tutto curato e gestito dalla ditta EPOX SRL)

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

l'Azienda 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.

Il Personale al momento dell'assunzione viene correttamente formato sui 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.

Gli interventi formativi possono avvenire:

- all'interno, a cura di CARAVATI GIAMPIERO o di altri soggetti esperti nella materia.

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.

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 30/03/2009 viene firmato in calce da:

- CARAVATI GIAMPIERO, in qualità di rappresentante legale dell'Azienda;

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

CANTELLO, 30/03/2009.

Firma del rappresentante
legale dell'Azienda