
Soggetto: Antonio SPEDICATO
Indirizzo: Via Amulio 13/15 00181 ROMA
P. IVA 02005980582
CCIAA di Roma N° 101499

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**
(D.Lgs. n. 196/2003)

Il presente documento si compone di n.15 pagine

Il titolare del trattamento

Antonio Spedicato

Il responsabile del trattamento

Antonio Spedicato

Il Signor Antonio SPEDICATO, esercente l'attività di commercio al dettaglio di strumenti musicali con sede in Roma, Via Amulio,13/15

Premesso

Che per lo sviluppo della semplice struttura aziendale e per l'omogeneità di dati trattati e del tipo di trattamento, l'attività è normalmente riconducibile alla gestione di dati personali comuni di clienti/fornitori e dipendenti inerenti l'attività di fatturazione e registrazione contabile;

con il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, fisiche e logiche, previste per la tutela dei dati trattati.

In conformità con quanto prescritto al punto 19 del Disciplinare tecnico(allegato B al D.Lgs.) nel presente documento si forniscono idonee informazioni riguardanti:

- 1). Elenco dei trattamenti di dati personali (punto 19.1) mediante:
 - 1.1) individuazione dei dati personali trattati;
 - 1.2) descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
 - 1.3) l'elaborazione della mappa dei trattamenti effettuati;
- 2) Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto19.2);
- 3) Analisi dei rischi a cui sono soggetti i dati (punto19.3);
- 4) Misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati(punto19.4);
- 5) Criteri e modalità di ripristino dei dati a seguito di distruzione o danneggiamento(punto 19.5);
- 6) Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno (punto 19.7);
- 7) Procedure per il controllo sullo stato della sicurezza;
- 8) Dichiarazioni d'impegno e firma

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 Tipologie di dati trattati

A seguito dell'analisi compiuta si sono identificati i seguenti atti e documenti trattati:

1. Trattamenti svolti dall'Area Amministrazione

- Trattamenti di dati comuni/sensibili/giudiziari/particolari dei dipendenti del Titolare, raccolti direttamente dall'interessato o da altre funzioni aziendali per finalità di predisposizione dei cedolini paga, obblighi di legge, esecuzione contratti di lavoro (**BD DIPENDENTI**)
- Trattamenti di dati comuni/sensibili/giudiziari/particolari dei dipendenti del Titolare raccolti direttamente dall'interessato per finalità di conservazione dei dati in ottemperanza agli obblighi di legge. (**BD DIPENDENTI**)
- Trattamenti di dati comuni dei Clienti per finalità contrattuali, contabili, amministrative (**BD CLIENTI**)
- Trattamenti dei dati dei clienti per finalità di Recupero Crediti (**BD CLIENTI**)

- Trattamenti di dati comuni dei Fornitori per finalità contrattuali, contabili, amministrative (**BD FORNITORI**)

2. Trattamenti svolti dall'Area Commerciale

- Trattamenti di dati comuni dei Clienti per finalità di promozione/vendita dei servizi (fax, catalogo, posta, telefono) anche mediante attività di marketing diretto. (**BD CLIENTI E POTENZIALI CLIENTI**)

3. Trattamenti svolti dall'Area Segreteria

- Trattamenti di dati comuni/sensibili/giudiziari/particolari dei dati di tutte le banche dati censite, dati trattati contenuti nella corrispondenza in entrata e in uscita del Titolare. La raccolta avviene direttamente dall'interessato o da altre funzioni aziendali (tramite posta ordinaria, e mail, fax) per finalità di protocollo. Si tratta prevalentemente di attività di mera consultazione svolta al fine di indirizzare correttamente la corrispondenza. (**Tutte le Banche Dati**)

1.2 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene nella sede e luogo di lavoro, situata in Via Amulio, 13/15, all'interno della quale è stata individuata un "open space" adibita alle operazioni di amministrazione, commerciale e di segreteria. Altra area di trattamento è situata al sottostante locale magazzino del negozio.

A -Schedari e altri supporti cartacei

I supporti cartacei sono raccolti in schedari a loro volta custoditi come segue:

- Archivio 1 localizzato in "Open space"ove in apposito scaffale, individuato con la lettera "A" vengono archiviati i supporti cartacei relativi ai trattamenti 1,2,3.
- Archivio 2 localizzato nel locale magazzino, sottostante il negozio, ove è stato individuato un piccolo locale con porta e serratura, individuato dalla lettera "B" e al quale accedono solo le persone autorizzate, dove vengono archiviati i supporti cartacei a fine ciclo lavorativo.

B - Elaboratori non in rete

Sono presenti n. 2 elaboratori (*stand alone*) tramite i quali si svolge parte del lavoro della struttura:

- Pc HP Pavillono localizzato nella "open space";
- Pc compatibile assemblato ubicato nel sottostante locale magazzino.

C - Elaboratori in rete privata

Il sistema di lavoro della struttura NON avviene con elaborazione in rete privata ma solo su postazioni fisse (*stand alone*) di cui al punto B.

D -Elaboratori in rete pubblica

Risulta collegato ad internet il seguenti PC: assemblato senza marca ubicato nell'area magazzino.

E - Impianti di video-sorveglianza

Al solo fine della tutela patrimoniale è utilizzato un impianto di video-sorveglianza resi necessario in quanto la porta di ingresso del negozio non è visibile dall'area "open space". L'impianto di cui trattasi è privo della funzione di **registrazione delle immagini** ed inquadra la sola merce esposta nel locale di vendita a ridosso della porta di accesso al negozio.

I soggetti che si trovano nella zona videosorvegliata sono avvertiti tramite apposito cartello esposto.

1.3 Mappa di trattamenti effettuati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delineano i seguenti schemi:

Tipologia di trattamento	Cartaceo	PC non in rete	PC in rete privata	PC in rete pubblica (internet)	Video sorveglianza
Trattamenti dell'area Amministrazione	X	X		X	
Trattamenti dell'area Commerciale	X	X		X	
Trattamenti dell'area segreteria	X	X		X	X

TRATTAMENTO		Natura dei dati trattati			Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati	
I T	Finalità perseguita o attività svolta	Categorie di BD interessati	C	S	G			
1	Trattamenti svolti dall'area amministrazione	CLIENTI FORNITORI DIPENDENTI	X	X		"open space" negozio	Commercialista Studio Cannizzaro Consulente del lavoro Studio Corbolotti	Pc + archivio cartaceo
2	Trattamenti svolti dall'area commerciale	CLIENTI	X			Negozi		Pc + Archivio Cartaceo
3	Trattamenti svolti dall'area segreteria	TUTTI	X	X		"open space" negozio		Archivio Cartaceo

Elenco dei trattamenti: descrizione degli strumenti utilizzati, personal computer

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supp.	Tipologia di dispositivi di accesso	Tipologia di interconnessione	PC utilizzati
1 – 3	BD Dipendenti BD Clienti BD Fornitori	"open space" negozio	Personal computer	"stand Alone"	HP Pavillon
3	BD Clienti BD Fornitori	Locale magazzino	Personal computer	"stand Alone" collegamento internet	Assemblato privo di marca
3	BD Clienti e potenziali	"open space" negozio	Personal computer	"Stand Alone"	HP Pavillon

Archivi cartacei

Identificativo del trattamento	Eventuale banca dati	Archivio Cartaceo	Localizzazione
1 – 2 – 3	Tutte	Raccoglitori Fascicoli schedari	"open space" scaffale lett.A. Archivio locale magazzino lett.B.

Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati emerge che:

- 1) solo i dati personali vengono trattati sistematicamente con supporti cartacei e con elaborazione;
- 2) i dati sensibili trattati con elaborazione, sono limitati a quelli necessari per assolvere agli obblighi normativi, contrattuali e specifici;
- 3) non si rilevano dati giudiziari trattati essi comunque non vengono trattati con elaborazione;
- 4) l'elaboratore in rete pubblica (internet) presente, non è collegato in rete con altri, e funziona esclusivamente "stand Alone".

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' ED INTERVENTI FORMATIVI DEGLI INCARICATI

Titolare del trattamento dei dati

Per il trattamento dei dati personali il titolare non ha nominato responsabili, assumendo direttamente l'incarico di progettare, realizzare e mantenere in efficienza le misure di sicurezza.

Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto dal Titolare, con il quale si individua l'ambito del trattamento consentito. Le lettere di incarico che vanno a completare il mansionario sono allegate al presente documento. (allegato B)

Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le maggiori cautele di trattamento che questo tipo di dati richiedono;
- modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornirne copia la Titolare;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;
- modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali;
- aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza;

Formazione degli incaricati al trattamento

Agli incaricati al trattamento, il titolare (direttamente o tramite soggetti da lui identificati) fornisce la necessaria formazione:

- al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansione;
- in occasione dell'introduzioni di nuovi strumenti e programmi informatici.

La formazione interesserà sia le norme generali in materia di privacy, sia gli aspetti peculiari dei trattamenti effettuati.

Competenze e responsabilità delle strutture preposte ai trattamenti

Per il trattamento dei dati personali sono previste le seguenti figure:

- 1) Titolare del trattamento dei dati: sig. Antonio SPEDICATO;
- 2) Responsabile del trattamento : sig. Antonio SPEDICATO;
- 3) Incaricato dei trattamenti di dati personali:
- sig. Sergio FRAIOLI, per quanto attiene le attività proprie dell'area commerciale.

Il trattamento dei dati, nell'ambito dell'organizzazione del lavoro in negozio, prevede una distribuzione di compiti e responsabilità come sotto riportata:

STRUTTURA	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Negozi	1 - 2	Il sig. Antonio Spedicato si occupa personalmente del trattamento dei dati relativi a tutte le attività di gestione dell'azienda; si occupa della trasmissione al Consulente del Lavoro dei dati relativi ai dipendenti dell'azienda ed all'archiviazione di tutta la documentazione relativa non trasmessa; si occupa della trasmissione al Commercialista dei dati relativi alla formalizzazione della contabilità aziendale; si occupa delle procedure di backup dei dati informatici. Il sig. Antonio SPEDICATO, titolare e responsabile del trattamento dei dati effettuato dall'incaricato, ne coordina e controlla l'opera.
Negozi	3	Il sig. Sergio FRAIOLI si occupa dell'attività riferita all'area commerciale ed ai relativi archivi Clienti, Potenziali clienti, Fornitori. Si occupa delle procedure di backup dei dati informatici.

3. ANALISI DEI RISCHI CUI SONO SOGGETTI I DATI

L'analisi dei possibili rischi che gravano sui dati è stata effettuata in relazione alla fonte che può generare il rischio, ossia classificandoli in base all'evento scatenante: rischi legati ai comportamenti degli operatori, connessi agli strumenti utilizzati e relativi al contesto fisico ambientale.

Comportamento degli operatori

Rischi	Si/no	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Sottrazione di credenziali di autenticazione (login e password)	NO	
Carenza di consapevolezza, disattenzione o incuria	SI	BASSA
Comportamenti sleali o fraudolenti	NO	
Errore materiale	SI	BASSA

Eventi relativi agli strumenti elettronici

Rischi	Si/no	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
--------	-------	--

	Azioni di virus informatici o di programmi suscettibili di recare danno	SI	BASSA
	Spamming o tecniche di sabotaggio	NO	
	Malfunzionamento, indisponibilità o degrado degli strumenti	SI	BASSA
	Accessi esterni non autorizzati	NO	
	Intercettazioni delle informazioni con utilizzo delle reti di connessione tra PC	NO	

Contesto fisico ambientale

Rischi		Si/n o	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
	Accessi non autorizzati a locali/reparti ad accesso ristretto	SI	BASSA
	Sottrazione di strumenti contenenti dati	SI	BASSA
	Eventi distruttivi, naturali od artificiali, nonché dolosi, accidentali o dovuti ad incuria	SI	BASSA
	Guasto ai sistemi complementari	SI	BASSA
	Errori umani nella gestione della sicurezza fisica	SI	BASSA

4. MISURE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

Alla luce dei fattori di rischio e delle aree individuate nel presente paragrafo vengono descritte le misure atte a garantire:

- la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito degli strumenti elettronici.

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- misure già adottate al momento della stesura del presente documento;
- ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

4.1 La protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio previsti dalla normativa vigente;
- impianto di condizionamento.

Sono adottate le seguenti misure per impedire accessi non autorizzati:

- Impianto anti intrusione ad ultrasuoni;
- Impianto sonoro di accesso al negozio.

4.2 Custodia e archiviazione dei dati

All'incaricato sono state impartite le istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- il corretto accesso ai dati personali, sensibili e giudiziari;
- la conservazione e la custodia di documenti, dati e supporti contenenti dati personali, sensibili e giuridici;
- la definizione delle persone autorizzate ad accedere ai locali archivio e le modalità di accesso;

4.3 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici
- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati possono accedere e utilizzare al fine delle proprie mansioni lavorative
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.

Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema;

Protezione di strumenti e dati

Premesso che non vengono trattati dati sensibili e giudiziari in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistema firewall anti-intrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.

All'incaricato è stato affidato il compito di aggiornare periodicamente, ogni 3 (tre) mesi il sistema di protezione.

Supporti rimovibili

Anche se le norme prevedono particolari cautele solo per i supporti rimovibili contenenti dati sensibili e giuridici, la tutela per il trattamento viene estesa ai dati personali come segue:

- custodia dei supporti in contenitori chiusi a chiave in locali con accesso ai soli autorizzati;
- cancellazione e/o distruzione del supporto una volta cessate le ragioni per la conservazione.

5. CRITERI E MODALITÀ' DI RIPRISTINO DATI

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema. Il salvataggio dei dati avviene:

- con frequenza giornaliera
- le copie vengono custodite in un luogo protetto locale magazzino lettera B.

6. AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nello svolgimento dell'attività, vengono affidati dati personali all'esterno

- Consulente del lavoro, studio Corbolotti;
- Commercialista Studio Cannizzaro.

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri degli impegni assunti per l'adozione delle misure
Preparazione delle buste paga ed assolvimento dei relativi obblighi di legge	Elaborazione delle buste paga dei dipendenti	Consulente del lavoro " Studio Corbolotti"	Studio professionale che ha attestato, al momento del conferimento dell'incarico, il rispetto di quanto previsto dalla normativa vigente sulla privacy
Tenuta delle scritture contabili, ed annessi adempimenti giuridici e fiscali	Clienti, fornitori, dipendenti, altri	Commercialista "Studio Cannizzaro"	Studio professionale che ha attestato, al momento del conferimento dell'incarico, il rispetto di quanto previsto dalla normativa vigente sulla privacy

7. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il titolare mantiene aggiornate le misure di sicurezza al fine di adottare gli strumenti più idonei per la tutela dei dati trattati. Egli verifica inoltre con frequenza mensile l'efficacia delle misure adottate relativamente a:

- accesso fisico a locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dati trattati;
- efficacia e utilizzo misure di sicurezza strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti magnetici non più riutilizzabili;
- livello di informazione degli interessati.

8. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data 29/03/2006 viene firmato in calce da Antonio SPEDICATO in qualità di titolare, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

L'originale del presente documento è custodito presso la sede della società, per essere esibito in caso di controllo.

Una copia verrà consegnata ai responsabili di determinati trattamenti di dati appositamente nominati.

29 marzo 2006-03-26