

Documento programmatico sulla sicurezza

Redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g) del D.Lgs. 196/2003 e del disciplinare tecnico (Allegato B del D.Lgs. n. 196/2003)

Il Signor [Andrea Pasini](#) esercente la professione di [Perito Industriale](#) con sede in Parma, Via [Sofia](#) n. [10/B](#)

Premesso che nell'ambito della propria attività effettua trattamento di dati personali, come di seguito elencati, 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:
Individuazione dei dati personali trattati;
Descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
L'elaborazione della mappa dei trattamenti effettuati;
2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (punto 19.2.);
3. Analisi dei rischi a cui sono soggetti i dati (punto 19.3.);
4. Misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati (punto 19.4.);
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 di firma.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Tipologie di dati trattati

A seguito dell'analisi compiuta si sono identificati i seguenti trattamenti:

- Dati relativi al personale o ai candidati per diventarlo, di natura anche sensibile;
- Dati comuni relativi a clienti e fornitori;
- Dati relativi allo svolgimento di attività economiche e commerciali.

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

Il trattamento dei dati avviene nella sede situata in edificio direzionale.
Gli uffici sono dislocati al piano quarto; l'accesso al piano è controllato da sistema di chiusura blindato, l'accesso al locale è controllato da sistema di videocitofono.

A- Schedari e altri supporti cartacei

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

- Archivio n. 1 localizzato nel locale "sala riunioni" ove, in appositi armadi, vengono archiviati i supporti cartacei di comune e continuo utilizzo;
- Archivio n. 2 localizzato nel server del sistema informatico al quale accedono solo le persone autorizzate, ove vengono archiviati i supporti cartacei a fine ciclo lavorativo;

B – Elaboratori non in rete

Non sono presenti postazioni fisse non accessibili da altri elaboratori.

C – Elaboratori in rete privata

Il sistema di lavoro della struttura avviene con elaborazione in rete privata.

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

- n. 1 server, localizzato nell'area ufficio;
- n. 3 postazioni di lavoro dislocate nell'area ufficio tecnico;
- n. 2 stampanti di cui n. 1 laser dislocate nell'area ufficio tecnico;
- n. 1 dispositivo di backup localizzato nell'ufficio amministrativo.

D – Elaboratori in rete pubblica

Non è presente una struttura che utilizza reti di telecomunicazioni pubbliche.

E – Impianti di videosorveglianza

Non sono utilizzati impianti di videosorveglianza.

Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia di trattamento	Cartaceo	PC no rete	PC in rete privata	PC in rete pubblica	Video-Sorvegl.
Dati comuni relativi a utenti/clienti	x	x			
Dati comuni relativi a fornitori	x				
Dati comuni relativi ad altri soggetti	x				
Dati biometrici relativi al personale					
Dati relativi allo svolg. Di att. economi che e commerciali	X	x			
Dati relativi al personale, candidati, anche sensibili					
Dati di natura anche sensibili		x			

relativi a clienti/utenti					
Dati idonei a rivelare lo stato di salute					
Dati di natura giudiziaria					

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 i supporti cartacei e con elaborazione;
- 2) i dati sensibili trattati con elaborazione, sono limitati a quelli necessari per assolvere agli obblighi normativi e contrattuali;
- 3) i dati giudiziari trattati sono quelli necessari per assolvere agli obblighi normativi e di legge; essi comunque non vengono trattati con elaborazione;
- 4) gli elaboratori in rete pubblica presenti, non sono collegati in rete con altri, dispongono esclusivamente del collegamento ad internet (oppure altre ipotesi).

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 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 di ogni singolo incaricato, 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 la archiviazione degli stessi;
- modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai dati in essi contenuti, nonché per fornire copia al preposto alla custodia della parola chiave;
- 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;
- altro....

Formazione degli incaricati al trattamento

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

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

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

3. ANALISI DEI RISCHI CUI SONO SOGGETTI I DATI

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

Strumenti impiegati nel trattamento

Sono stati individuati come sorgenti soggette a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

Strumenti	Legenda
Schedari ed altri supporti cartacei custoditi nell'area controllata	A
Elaboratori non in rete custoditi nell'area controllata	B
Elaboratori in rete privata custoditi nell'area controllata	C
Elaboratori in rete pubblica	D

Fattori di rischio	Basso	Medio	Elevato
Rischio d'area legato all'accesso non autorizzato nei locali			A C
Rischio guasti tecnici hardware, software, supporti		C	
Rischio penetrazione nelle reti di comunicazione			
Rischio legato ad errori umani	A		C
Rischio d'area per possibili eventi distruttivi			A C

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 sono 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:

- impianto di condizionamento
- - operazioni di back up automatiche

Sono adottate le seguenti misure per impedire accessi non autorizzati (*elencare*):

- impianto di videocitofono
- porta di accesso agli uffici blindata.

4.2 Custodia e archiviazione dei dati

Agli incaricati sono state impartite 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, atti 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.
- Salvataggio in back up automatico dei dati.

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 antintrusione. Il sistema è altresì impostato per l'aggiornamento periodico automatico di protezione.

Agli incaricati è stato affidato il compito di aggiornare periodicamente, con cadenza semestrale, 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 MODALITA' 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

6. AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

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

7. CONTROLLO GENERALE SULLO STATO DELLA SICUREZZA

Il titolare (il responsabile per la sicurezza 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 almeno 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 back up
- distruzione dei supporti magnetici non più riutilizzabili
- livello di informazione degli interessati

8. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data 31 marzo 2006 viene firmato in calce da Andrea Pasini 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.

Parma, 31 marzo 2006

Firma del Titolare

.....

Allegato A

ORGANIGRAMMA PRIVACY

TITOLARE DEI DATI	
RESPONSABILI Andrea Pasini	INCARICATI AL TRATTAMENTO Matteo Groppi Michele Sivelli Mara Marozza

