

## 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)

### **Titolare del trattamento:**

Il dott. Alberto Barbiero, in qualità di libero professionista, esercitante attività di consulenza amministrativo-gestionale per soggetti pubblici e privati, operante occasionalmente trattamento di dati personali di persone fisiche e giuridiche nell'ambito della propria attività e pertanto configurabile come Titolare, con domicilio in Casalecchio di Reno (BO) in Via Caravaggio, 11 (domicilio fiscale).

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:

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 ( 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 firma

### **1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI**

#### **1.1 Tipologie di dati trattati**

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

- dati comuni dei clienti, dei fornitori o di terzi ricavati da albi, elenchi pubblici, visure camerali;
- dati comuni di eventuali collaboratori o di altri professionisti operanti in network, quali quelli necessari alle relazioni di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria;

- dati comuni dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati, compresi i dati sul patrimonio e sulla situazione economica, o necessari per fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi;
- dati comuni di terzi, forniti dai clienti per l'espletamento degli incarichi affidati, compresi i dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o afferenti alla reperibilità ed alla corrispondenza con gli stessi, o per atti giudiziari;
- dati comuni dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria;
- dati comuni di altri professionisti cui lo studio può eventualmente affidare incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria;
- dati giudiziari dei clienti, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;
- dati giudiziari di terzi idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato;
- dati sensibili dei clienti, dagli stessi forniti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico;
- dati sensibili dei clienti, dagli stessi forniti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute;
- dati sensibili di terzi, forniti dai clienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute.

## **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 presso lo stesso domicilio fiscale.

I locali sono all'interno di appartamento privato, ad accesso controllato e con sistema di sicurezza.

### **A - Schedari e altri supporti cartacei**

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

- Archivio 1 localizzato presso lo stesso domicilio fiscale ed operativo, ove in appositi armadi vengono archiviati i supporti cartacei di comune e continuo utilizzo;
- Archivio 2 localizzato presso lo stesso domicilio fiscale ed operativo, ove in appositi armadi e in locale al quale accedono solo le persone autorizzate vengono archiviati i supporti cartacei a fine ciclo lavorativo.

### **B - Elaboratori non in rete**

Un PC in postazione fissa è utilizzabile anche come elaboratore non in rete. Il PC è dislocato nell'area ufficio.

### **C - Elaboratori in rete privata**

Il sistema di lavoro della struttura avviene con elaborazione in rete pubblica

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

- N. 1 postazioni lavoro dislocate nell'area ufficio
- N. 1 elaboratore trasportabile al di fuori della sede d'ufficio (non contenente dati personali).
- N. 1 stampanti dislocate nell'area ufficio
- N. 1 dispositivo di backup localizzato nell'area ufficio

### **D - Elaboratori in rete pubblica**

Sono collegati ad internet i seguenti PC:

n. 1 PC fisso dislocati nell'area ufficio.

E' collegabile alla rete, mediante scheda di accesso autonoma, n. 1 PC portatile (non utilizzato per trattare dai dei clienti/fornitori/di terzi relativi all'attività).

### E - Impianti di video-sorveglianza

Non sono utilizzati impianti di video-sorveglianza

### 1.3 Mappa di trattamenti effettuati

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

Tipologia trattamento	Cartaceo	PC non in rete	PC in rete privata	PC in rete pubblica	Video Sorveglianza
Dati comuni relativi a clienti/utenti	X	X	X		
Dati comuni relativi a fornitori	X		X		
Dati comuni relativi ad altri soggetti	X		X	X	
Dati biometrici relativi a clienti/personale					
Dati idonei a rilevare la posizione di persone/oggetti					
Dati relativi allo svolgimento di att. econom./comm.	X		X		
Dati di natura giudiziaria	X	X			
Dati relativi al personale, candidati, anche sensibili	X				
Dati di natura anche sensibile relativi a clienti/utenti	X		X		
Dati idonei a rilevare lo stato di salute	X				

### 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 e contrattuali;
- 3) i dati giudiziari trattati sono quelli necessari per assolvere agli obblighi normativi e di Legge;
- 4) gli elaboratori in rete pubblica presenti, non sono collegati in rete con altri, dispongono esclusivamente del collegamento a 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 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 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 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 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;

### Formazione degli incaricati al trattamento

Agli incaricati al trattamento, il titolare (direttamente o tramite soggetti da lui identificati) fornisce la necessaria formazione al momento del conferimento dell'incarico comportante il trattamento di dati personali.

La formazione interesserà sia le norme generali in materia di privacy, sia gli 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 e 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 B C D

Rischio guasti tecnici hardware, software, supporti		<b>C D</b>	<b>B</b>
Rischio penetrazione nelle reti di comunicazione			<b>D</b>
Rischio legato ad errori umani	<b>A</b>	<b>B</b>	<b>C D</b>
Rischio d'area per possibili eventi distruttivi			<b>A B C D</b>

#### **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
- gruppo di continuità dell'alimentazione elettrica
- impianto di condizionamento

Sono adottate le seguenti misure per impedire accessi non autorizzati:

- a) accesso controllato;
- b) comunicazione preventiva per riconoscimento prima dell'accesso.

##### **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
- la password è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti

agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi.

- autorizzazione e definizione delle tipologie di dati ai quali gli incaricati posso 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.

Agli incaricati è stato, comunque ed in ogni caso, affidato il compito di aggiornare a cadenza almeno 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 settimanale
- le copie vengono custodite in un luogo protetto

### **6. AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO**

Nello svolgimento dell'attività, **vengono/non vengono** affidati dati personali all'esterno (*nel caso il trattamento venga affidato all'esterno sono state impartite istruzioni per iscritto al terzo destinatario, al fine di rispettare quanto prescritto dal codice della privacy*)

### **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 backup
- distruzione dei supporti magnetici non più riutilizzabili
- livello di informazione degli interessati

#### **8. DICHIARAZIONE D'IMPEGNO E FIRMA**

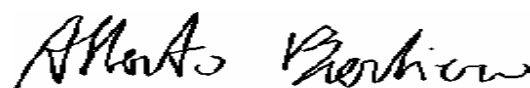
Il presente documento redatto in data 27 marzo 2006 viene firmato in calce da Alberto Barbiero in qualità di titolare del trattamento, e verrà aggiornato periodicamente entro il 31 marzo di ogni anno.

L'originale del presente documento è custodito presso il domicilio fiscale e operativo, per essere esibito in caso di controllo.

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

Casalecchio di Reno, 27 marzo 2006

Firma del Titolare



**Allegato A**

**ORGANIGRAMMA PRIVACY**

<b>Titolare del trattamento</b>	<b>Responsabile del trattamento</b>	<b>Incaricati e qualifica</b>

## **Allegato B**

### **LETTERA DI INCARICO**

Il sottoscritto \_\_\_\_\_ in qualità di Titolare/Responsabile del trattamento dei dati dello Studio Legale \_\_\_\_\_ sito in \_\_\_\_\_

#### **INCARICA**

il Dr./sig./la sig.ra \_\_\_\_\_ nato/a a \_\_\_\_\_ il \_\_\_\_\_ al trattamento dei dati (personali / sensibili / giudiziari : specificare) nell'ambito delle funzioni di \_\_\_\_\_ (legale, praticantato, segreteria) che è chiamato/a a svolgere presso questo Studio.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile in generale ed elencate nel d.p.s.

Per ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:

- a) divieto di comunicazione o diffusione dei dati senza la preventiva autorizzazione del Titolare/Responsabile;
- b) l'accesso ai dati è autorizzato limitatamente all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
- c) la fase di trattamento dei dati dovrà essere preceduta dalla informativa al cliente in forma scritta e dal consenso di quest'ultimo al trattamento nei casi previsti dalla legge;
- d) in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- e) le proprie credenziali di autenticazione sono strettamente personali e devono rimanere riservate. Tali credenziali sono univocamente associate all'incarico al quale sono state fornite.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Qualsiasi altra istruzione può essere fornita dal Titolare che provvede anche alla formazione degli incaricati.

Per ogni altra misura qui non prevista si fa riferimento al documento programmatico sulla sicurezza adottato dallo Studio.

#### **TRATTAMENTO CONSENTITO**

- a) raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- b) qualsiasi accesso e trattamento espressamente previsto e descritto nel d.p.s.;
- c) qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Data e luogo

Il responsabile del trattamento

L'incaricato

\_\_\_\_\_

\_\_\_\_\_

## **Allegato C**

### **Dichiarazione di conformità alle misure minime di sicurezza**

*(nel caso di affidamento di incarico a persone/società esterne quest'ultime devono rilasciare dichiarazione di conformità alle misure minime di sicurezza)*

Il/La sottoscritto/a (società), al/alla quale è stato affidato il trattamento è consapevole che i dati personali sono soggetti all'applicazione del D. Lgs 196/2003.

Egli/Essa dichiara di aver adottato le misure minime di sicurezza previste dagli artt. 33 – 36 del D. Lgs. 196/2003, e di effettuare il trattamento dei dati con le seguenti modalità:  
\_\_\_\_\_ (con/senza strumenti elettronici)

Il/La sottoscritto/a (società) relaziona annualmente lo studio legale sulle misure di sicurezza adottate. Il titolare dello Studio ha il diritto di verificare periodicamente l'effettiva adozione delle misure di sicurezza presso la nostra struttura.

Il/La sottoscritto/a (società) è autorizzato/a al trattamento dei dati relativi a \_\_\_\_\_ (definire quale/i trattamenti) in nome e per conto del titolare \_\_\_\_\_ dello studio legale \_\_\_\_\_ (riportare tutti i dati).

Firma \_\_\_\_\_