# DOCUMENTO PROGRAMMATICO

# SULLA SICUREZZA

EDIL BRIANZA DI BELLOTTI FILIPPO & C. SNC

**MARZO 2009**

**Il Responsabile della Privacy**

**BELLOTTI FILIPPO**

# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Ai sensi e per gli effetti dell'art.34 del Decreto Legislativo n.196/2003 e del disciplinare tecnico ad esso allegato si redige il seguente Documento Programmatico sulla Sicurezza dei dati.

**Data ultima stesura** **MARZO 2009**

Redatto da Il Responsabile della Privacy **BELLOTTI FILIPPO**

**DATI AZIENDA**

Soggetto/Azienda EDIL BRIANZA DI BELLOTTI FILIPPO & C. SNC

Indirizzo VIA MAZZINI , 3

Città AROSIO CAP 22060 Prov COMO

Codice Fiscale Partita IVA 00255720138

Telefono: 031-761020 Fax 031-761020

E_Mail: edil.brianza@tin.it

## ATTIVITA' COSTRUZIONI E RISTRUTTURAZIONI CIVILI E INDUSTRIALI

**Numero dipendenti …….8.……

**Numero computer …….2..…

**Numero server ……..1.…

**Accesso ad Internet SI

Il documento ha lo scopo di identificare, attraverso una puntuale analisi dei rischi, le misure di sicurezza fisiche, logiche ed organizzative adottate o da adottare per la sicurezza e l'integrità degli archivi aziendali, organizzati su supporto cartaceo od automatizzato che contengono dati personali soggetti all'applicazione del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in Materia di Protezione dei dati personali".

Le misure individuate sono tali da soddisfare i requisiti descritti nell'Allegato B dello stesso Decreto Legislativo 30 giugno 2003, n. 196 "Disciplinare Tecnico in materia di misure minime di sicurezza (art. 33-36 del Codice)

Nel seguito i termini Titolare, Responsabile, Incaricato, Amministratore di sistema, Preposto, Trattamento, Dato personale e Dato particolare (o sensibile) sono usati in conformità alle definizioni del Codice citato.

.

# 2 Aspetti generali.

## 2.1 Contenuti.

L'Azienda Titolare, in collaborazione con i Responsabili individuati, intende sviluppare il programma di sicurezza in modo adeguato secondo quanto indicato nel presente documento allo scopo di:

- ❖ minimizzare le probabilità di appropriazione, danneggiamento o distruzione, anche involontaria, di apparecchiature informatiche, archivi informatici o cartacei contenenti dati personali o comunque critici per il business aziendale;
    - **minimizzare le probabilità di accesso alle informazioni personali o modifiche non autorizzate.**

## 2.2 Applicabilità.

Le prescrizioni descritte nel presente documento si applicano a tutti i trattamenti eseguiti nell'ambito dell'intera struttura organizzativa della società e sono da considerare vincolanti nei rapporti contrattuali relativi a trattamenti eseguiti anche da altri soggetti esterni cui sia conferito un incarico di Responsabile del trattamento di dati e di cui la Società sia Titolare.

## 2.3 Revisioni.

Il presente documento è valido per **un anno** dalla data della sua emissione o della sua ultima revisione.

Si procede con una revisione del documento:

- **alla scadenza del periodo di validità, con lo scopo di valutare l'adeguatezza del documento anche in considerazione dell'evoluzione tecnologica;**
- **ogni qualvolta dovessero cambiare le strutture di dati o le sedi operative, presso cui possono essere trattati i dati , e gli strumenti (PC, supporti informatici, archivi cartacei);**
- **ad ogni modifica della struttura organizzativa cui è demandata la responsabilità della sicurezza;**
- **ad ogni controllo periodico cui le misure di sicurezza sono sottoposte per verificarne la validità ed efficacia. In tal caso la revisione del documento riporterà gli esiti di tale controllo ed eventuali riferimenti alla documentazione prodotta.**

La nuova versione del documento riporterà, in modo sintetico, un verbale del processo di revisione che ha portato alla sua emissione con l'indicazione delle motivazioni (All.).

## 2.4 Compiti e responsabilità.

Sono definiti i seguenti ruoli, compiti ed incarichi con le responsabilità indicate:

### 2.4.1 Titolare del trattamento di dati personali.

Titolare del trattamento è la società

**EDILBRIANZA DI BELLOTTI FILIPPO E C SNC**

### 2.4.2 Responsabile della Privacy

Mediante comunicazione scritta è stata nominata Responsabile della Privacy

**BELLOTTI FILIPPO**

### 2.4.3 Incaricati interni del trattamento di dati personali (sensibili e non).

Gli operatori che trattano dati personali (sensibili e non) sono incaricati mediante comunicazione scritta, con:

- l'assegnazione di compiti e responsabilità;
- l'utilizzo di un sistema di abilitazioni che limita l'accesso ai soli dati e trattamenti necessari all'espletamento della normale attività lavorativa;

Mediante comunicazione scritta sono stati nominati Incaricati al trattamento dei dati

**PROSERPIO FULVIA – BELLOTTI FILIPPO – COLZANI GIANLUCA**

### 2.4.4 Amministratore di sistema e Responsabile dei Sistemi Informativi

**Il Responsabile della Privacy che a sua volta incarica un soggetto esterno per gli interventi necessari.**

Gli interventi vengono verbalizzati da azienda incaricata dal Responsabile.

## 3 Definizione dei trattamenti eseguiti

Presso la Società vengono eseguiti i trattamenti previsti dal "Codice in Materia di Protezione dei dati personali" e cioè operazioni o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

Le finalità e le modalità del trattamento sono quelle previste dalla vigente normativa, nonché dalla informativa fornita a tutti gli interessati.

## 4 Identificazione delle risorse da sottoporre alle misure di sicurezza.

La Società ha proceduto all'individuazione e definizione delle risorse da sottoporre alle misure di sicurezza di seguito riportate.

**Definizione delle risorse critiche**
Sono definiti i seguenti tipi di risorse critiche:

- **Archivi cartacei o informatici su pc, conservati presso la società o ai quali si ha comunque accesso**
- **Elaboratori, sistemi automatizzati o strumenti per l'elaborazione delle informazioni contenute negli archivi di cui sopra**
- **Software utilizzato per il trattamento**
- **Supporti informatici e non, che contengono i dati, i documenti o loro copie**
- **Locali, edifici, strutture logistiche o mezzi di trasporto che ospitano, anche temporaneamente gli archivi**
- **Archivi**

Si sono stati individuati i seguenti archivi:

| Archivio/Dati | Dati critici per il business | Dati personali | Dati sensibili |
|---|---|---|---|
| Contabilità | SI | SI | SI |
| Archiviazione documenti | SI | SI | SI |
| Rubrica telefonica e fax | SI | SI | SI |

| | |
|---|---|
| Dati critici per il business: | Sono compresi in questa categoria tutti i dati la cui assenza o carenza rappresentano una criticità per il business aziendale. |
| Dati personali: | Sono compresi in questa categoria tutti i dati che, compresi o meno tra quelli critici, realizzano il trattamento di Dati personali così come definiti dal "Codice in Materia di Protezione dei dati personali". |
| Dati sensibili : | Sono compresi in questa categoria il sottoinsieme della precedente categoria che tratta i dati relativi alla sfera personale quali ad esempio quelli relativi alla salute, alla vita sessuale, (eventualmente alle opinioni religiose, politiche, sindacali, filosofiche, origine etnica). |

## 5 Prescrizioni di sicurezza.

In considerazione delle risorse critiche e dei rischi individuati, vengono descritte le misure di sicurezza Fisiche, Logiche ed Organizzative che sono state adottate.

Le misure sono tali da rispettare gli obblighi previsti dal “Codice in Materia di Protezione dei dati personali” e dai suoi allegati.

### 5.1 Misure fisiche.

Segue dettaglio delle misure fisiche predisposte al fine di ottemperare ai dettami normativi in merito alla protezione dei dati personali.

**5.1.1.Controllo accessi.** In merito al controllo accessi è predisposto quanto segue.

Per i dipendenti e collaboratori è possibile accedere agli uffici quotidianamente e l’accesso è protetto da antifurto.

I visitatori possono accedere agli uffici solo se espressamente autorizzati dal personale della società.

**5.1.2. Controllo accessi ad aree e locali del trattamento automatizzato.**

L’accesso alle aree e locali del trattamento automatizzato è protetto.

**5.1.3. Controllo accessi agli archivi cartacei.** Gli archivi cartacei sono custoditi sotto chiave presso l’amministrazione e l’accesso è consentito solo agli Incaricati espressamente autorizzati.

**5.1.4. Sistema antincendio.** La Società ha proceduto ad un’attenta verifica dei sistemi antincendio verificando quanto al seguito.

I locali sono protetti da un sistema antincendio adeguato allo scopo, efficiente e rispondente alla normativa vigente. Tale sistema viene sottoposto a regolare manutenzione sulla base dei vigenti dettami normativi.

### 5.2 Misure logiche.

Segue dettaglio delle misure logiche predisposte dalla Società al fine di ottemperare ai dettami normativi in merito alla protezione dei dati personali.

**5.2.1. Identificazione ed Autenticazione degli utenti**.

Al fine di garantire la sicurezza nel trattamento dei dati personali la società ha provveduto a predisporre e mettere in atto quanto al seguito.

**5.2.2. Codice identificativo (User-id).**

A tutti gli Incaricati del trattamento di dati personali viene attribuita un codice personale per l'utilizzo del PC. Lo stesso codice non può essere assegnato a persone diverse, neppure in tempi diversi.

In caso di revoca dell'Incarico e/o dell'autorizzazione il codice identificativo viene reso immediatamente inutilizzabile.

**5.2.3. Parola chiave (Password).**

Ad ogni codice identificativo è associata una parola chiave per l'utilizzo dell'elaboratore, che viene contestualmente comunicata dal preposto alla custodia delle parole chiave.

Al primo utilizzo, l'incaricato ha l'obbligo di modificarla tenendo presenti le seguenti regole:

- **deve essere alfanumerica, di lunghezza non meno di 8 caratteri, di cui almeno 1 numerico e non deve fare riferimento a date e/o nomi che possano essere collegati all'intestatario del codice identificativo (user-id);**
- **non deve essere composta utilizzando lo user-id;**
- **non deve essere ottenuta anagrammando la precedente;**
- **deve essere sostituita almeno ogni 3 mesi se si accede a dati sensibili, O OGNI 6 MESI PER TUTTI GLI ALTRI TIPI DI DATI.**
- **non deve essere comunicata ad altri, anche per il solo utilizzo temporaneo o in caso di emergenza se non dietro esplicito intervento del Preposto alla custodia delle parole chiave;**
- **non deve essere trascritta su carta né memorizzata su supporto magnetico.**

Alcune stazioni di lavoro utilizzate per l'accesso ai dati personali sono dotate di screen saver protetti da password. E' quindi inibito un loro utilizzo improprio in caso di abbandono, anche temporaneo, della stazione già abilitata all'accesso.

**5.2.4. Autorizzazioni all'accesso e Profili Utente.**

Vengono definiti i compiti di ciascun Incaricato: ad ogni user-id attribuita a ciascun incaricato vengono assegnate le abilitazioni all'accesso che competono al profilo utente individuato dalla comunicazione di incarico.

(Nel caso di trattamento di dati sensibili, la comunicazione di incarico è accompagnata da una specifica autorizzazione, la cui validità è verificata periodicamente, e comunque, almeno una volta l'anno).

**5.2.5. Criteri e Procedure di rilascio di user-id e password.** Esiste una procedura per la generazione delle password ai vari sistemi quando un nuovo utente prende servizio .

In caso di revoca dell'incarico e/o dell'autorizzazione il codice identificativo viene reso immediatamente inutilizzabile. L'Amministratore di sistema ed il Responsabile custodia password vi provvedono nel momento in cui l'utente cessa l'attività.

E' prevista la disattivazione della user-id in caso di perdita della qualità che consente l'accesso all'elaboratore o in caso di mancato utilizzo per un periodo superiore ai sei mesi.

L’Amministratore di sistema ha il compito di vigilare sull’applicazione di tali criteri.

### 5.2.6. Criteri e Procedure di controllo degli accessi agli archivi informatici.

L’accesso agli archivi informatici è controllato da un apposito sistema di controllo che, sulla base delle abilitazioni corrispondenti ai vari settori di appartenenza, consente l’accesso ai soli elaboratori, archivi e dati necessari e sufficienti per il trattamento.

L’Amministratore di sistema ha il compito di vigilare sul corretto utilizzo delle procedure previste.

### 5.2.7. Criteri e Procedure di controllo accessi agli archivi cartacei.

L’accesso agli archivi cartacei è controllato e selezionato sulla base della necessità del trattamento.

Se gli incaricati prelevano documenti devono conservarli e restituirli al termine delle operazioni affidate.

Gli archivi contenenti dati sensibili sono conservati in contenitori muniti di serratura.

### 5.2.8. Controllo accessi.

Gli accessi alla rete, ai sistemi di elaborazione, ai programmi applicativi, ai dati sono protetti contro le intrusioni da uno specifico sistema di controllo sia verso l’interno che verso l’esterno.

Ogni utente è abilitato all’accesso alle risorse di elaborazione necessarie per i trattamenti cui è autorizzato dal proprio settore di appartenenza.

### 5.2.9. Protezione antivirus.

Tutti gli elaboratori per i quali è applicabile sono protetti contro il rischio di intrusione ad opera di programmi di cui all’art 615- quinques del Codice Penale *(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni*).

La protezione avviene mediante l’utilizzo di adeguati programmi antivirus il cui aggiornamento avviene automaticamente ed in tempo reale (internet) dal sistema stesso.

Periodicamente si verifica l’efficacia della protezione antivirus mediante l’utilizzo di alcuni file danneggiati con i virus più recenti.

Il personale non può inibire l’operatività dei programmi antivirus installati.

### 5.2.10. Autorizzazioni degli strumenti.

Tutti gli strumenti utilizzabili per trattamento di dati personali sono abilitati dall’amministratore di sistema.

L’acquisto di hardware e software è approvato preventivamente dal Responsabile.

### 5.3 Misure Organizzative.

Segue dettaglio delle misure organizzative predisposte al fine di ottemperare ai dettami normativi in merito alla protezione dei dati personali.

#### 5.3.1. Comunicazione di incarico ed autorizzazione.

La società ha predisposto apposite procedure che prevedono per ogni figura (operatori, addetti ed outsourcing) coinvolta nel trattamento di dati personali l'assegnazione scritta di incarichi e responsabilità. Di tali comunicazioni viene tenuta storia controfirmata per accettazione e presa visione.

#### 5.3.2.Incaricati interni.

Tutti gli operatori che trattano dati personali vengono incaricati tramite comunicazione scritta. Questa definisce gli archivi e i dati cui l'incaricato ha accesso, le operazioni di trattamento consentite e identifica un profilo utente che definisce le abilitazioni nel sistema di controllo accessi agli archivi informatici. Viene data in modo esplicito anche l'autorizzazione al trattamento di dati sensibili.

#### 5.3.3.Trattamenti affidati a consulenti ed Aziende esterne.

Nel caso di ricorso a lavoratori, professionisti ed aziende esterne per il trattamento di dati personali (outsourcing) si procede, tenendo conto del tipo di servizio offerto, alla nomina di:

| | |
|---|---|
| **Incaricato:** | Qualora il servizio venga prestato sotto la direzione funzionale ed all'interno delle strutture |
| **Terzo responsabile:** | in tutti gli altri casi congiuntamente all'accettazione dell'incarico viene richiesta, quale documentazione delle misure adottate, copia del "**Documento Programmatico sulla Sicurezza**" che viene conservata assieme al presente documento. |

#### 5.3.4.Criteri e Procedure per il riutilizzo di supporti.

Tutti i supporti magnetici utilizzati devono essere inizializzati prima del loro utilizzo mediante apposite procedure indicate dal Responsabile che consentano di rendere illeggibili i dati precedentemente registrati. Tali procedure si applicano anche in caso di eliminazione dei supporti magnetici.

Tutti i supporti cartacei sui quali vengano prodotte stampe da archivi informatici oppure ottenuti attraverso la fotocopia di documenti relativi agli archivi aziendali, sono conservati dagli incaricati in contenitori muniti di serratura e, quando non più utilizzati, distrutti mediante un sistema che non consenta la lettura delle informazioni.

### 5.3.5.Criteri e Procedure per assicurare l’integrità dei dati.

I dati relativi agli archivi aziendali sono protetti contro il rischio di perdita, anche accidentale, attraverso apposite procedure che consentono il veloce ripristino delle informazioni perdute o danneggiate.

Tali procedure consentono il ripristino della correttezza delle informazioni con una perdita di dati non superiore all’ultima giornata lavorativa.

A tale scopo vengono prodotte le necessarie copie contestuali degli archivi .

Le prove di ripristino vengono effettuate almeno ogni sei mesi.

I supporti di backup sono conservati in un locale diverso da quello dove vengono elaborati.

La periodicità dei salvataggi, numero di versioni conservate e procedure di ripristino sono state definite in modo da soddisfare alle esigenza di sicurezza e sono estese a tutti gli archivi.

Le procedure consentono il ripristino selettivo dei soli dati danneggiati.

La società vieta agli utenti di installare programmi, immagini o comunque copiare file di qualunque tipo e provenienza sulla propria stazione di lavoro. Se ciò fosse necessario per lo svolgimento delle mansioni aziendali gli utenti devono rivolgersi ad un gestore dei sistemi informatici.

Gli elaboratori che potrebbero essere causa primaria di perdita o deterioramento dell’integrità di dati sono stati dotati di gruppo di continuità. L’efficienza di tali dispositivi viene testata periodicamente.

### 5.3.6.Criteri e Procedure per assicurare la disponibilità del servizio.

Le caratteristiche del servizio erogato dai sistemi informatici e la perdita di immagine, economica e di tempo che deriverebbe da una sua interruzione prolungata fanno ritenere necessaria la predisposizione di un piano per assicurare la disponibilità del servizio.

Tale piano di continuità, descritto in un apposito documento, deve avere le seguenti caratteristiche:

- Garantire la continuità del servizio relativamente almeno alle applicazioni individuate come critiche
- Consentire la ripresa del servizio entro il giorno lavorativo successivo

La funzionalità del piano viene verificata e collaudata almeno una volta ogni anno.

### 5.3.7.Criteri e Procedure per assicurare un uso dei dati corretto e conforme alle finalità della raccolta.

Il “Codice in Materia di Protezione dei dati personali” prevede che i dati personali oggetto del trattamento siano custoditi e controllati in modo da ridurre al minimo, oltre ai rischi già esaminati di distruzione, perdita, accesso non autorizzato, anche quelli legati ad un trattamento non autorizzato o ad un uso non conforme alle finalità dei trattamenti descritte precedentemente.

A tale scopo vengono adottate le misure riportate di seguito.

## 6 Verifica della congruenza dei fini.

Periodicamente, e comunque ad ogni revisione del presente documento, il Responsabile verifica che il trattamento eseguito sia in linea con quanto dichiarato dal Titolare. In caso di difformità, informa il

Titolare in modo da procedere a modificare la descrizione delle finalità e delle modalità del trattamento e provvedendo quando necessario a:

- correggere il trattamento scorretto
- richiedere il consenso al trattamento dei dati
- dare seguito alla eventuale comunicazione al Garante.

### 6.1 Verifica della scadenza.

Quando vengono a cessare gli scopi per i quali i dati sono stati raccolti o successivamente trattati secondo le finalità del trattamento, essi vengono cancellati.

Periodicamente e comunque ogni anno, viene effettuata una verifica affinché negli archivi non risultino memorizzati dati non più necessari al trattamento.

### 6.2 Verifica dell' attuazione dei diritti dell'interessato.

Il Responsabile garantisce l'attuazione di quanto necessario per garantire i diritti dell'interessato espressamente indicati agli art. 7-8 del "Codice in Materia di Protezione dei dati personali" attraverso una verifica periodica della procedura avente lo scopo di ottenere, senza ritardo, le seguenti azioni e/o informazioni in favore dell'interessato:

- **La conferma dell'esistenza o meno di dati personali che lo riguardino e la comunicazione in forma intelligibile dei medesimi dati, della loro origine, della logica e della finalità del trattamento**
- **La cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge**
- **L'aggiornamento, la rettifica ovvero, qualora vi abbia interesse, l'integrazione dei dati**
- **L'attestazione che le eventuali modifiche ed il loro contenuto sono portate a conoscenza di coloro ai quali i dati sono stati comunicati e/o diffusi.**

## 7 Piano di formazione.

Ai punti 2, 3, 4, 5 e 6 del presente documento deve essere data la massima diffusione. Per tale ragione esso viene consegnato ad ogni incaricato contestualmente alla comunicazione scritta di incarico.

Ad ogni revisione del documento e, comunque, ogni anno, tutti gli incaricati vengono istruiti sui rischi connessi al trattamento e sulle misure adottate per prevenire i possibili danni.

## 8 Elenco distribuzione. Segue elenco di distribuzione del presente documento

**Vengono effettuati controlli periodici sull'applicazione delle disposizioni contenute nel presente documento o ad esso relative**

**Il presente documento è redatto ai sensi del d.lgs 196/2003 e del relativo disciplinare tecnico, è aggiornato a MARZO 2009**

**Il Titolare del trattamento** **Il Responsabile della Privacy**

**ALLEGATI**
**LETTERE DI NOMINA:**
**Responsabile**
**IncaricatI**