DUEMILAUNO AGENZIA SOCIALE
società cooperativa sociale - ONLUS

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)

VERSIONE N.5 – marzo 2009

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da DUEMILAUNO AGENZIA SOCIALE società cooperativa sociale - ONLUS, con sede legale in Muggia, Trieste, via Colombara di Vignano n. 3, partita IVA n. 00767240328 (nel seguito del documento indicato come Titolare).

Conformemente a quanto prescrive il punto 19 del Disciplinare tecnico, allegato sub b) al D.Lgs 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:

1. l'elenco dei trattamenti di dati personali mediante:
   - la individuazione dei tipi di dati personali trattati
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti
   - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati e previsione di interventi formativi degli incaricati del trattamento
3. l'analisi dei rischi che incombono sui dati
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento
6. le procedure da seguire per il controllo sullo stato della sicurezza
7. dichiarazioni d'impegno e firma.

1. L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:

- si individuano i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili, distinguendo nell'ambito di questi ultimi quelli idonei a rivelare lo stato di salute e la vita sessuale, nonché quelli idonei a rivelare l'affezione da virus HIV e quelli di natura genetica) ed alla categoria di soggetti cui essi si riferiscono (clienti, fornitori, utenti, pazienti, personale…..)
- si descrivono le aree, i locali e gli strumenti con i quali si effettuano i trattamenti
- si elabora la mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti.

1.1 Tipologie di dati trattati

I dati trattati dal Titolare si possono suddividere come segue:

1 - Dati comuni relativi a clienti / utenti / consumatori
2 - Dati comuni relativi a fornitori
3 - Dati comuni relativi ad altri soggetti
4 - Dati relativi ai soci ed ai dipendenti, nonché ai candidati per diventarlo, di natura anche sensibile
5 - Dati di natura anche sensibile relativi a clienti / utenti
6 Dati idonei a rivelare lo stato di salute e/o la vita sessuale di clienti/utenti
7 - Dati idonei a rivelare l'affezione da virus HIV

1.2 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

I locali in cui vengono trattati dati personali e sensibili si possono dividere in due macro aree. La prima comprende la sede legale ed i vari uffici distaccati. Questi locali hanno quindi prettamente vocazione gestionale/amministrativa, dove di norma non è previsto l'accesso degli utenti dei servizi gestiti dalla cooperativa, se non in casi eccezionali e sporadici. Il trattamento dei dati personali può avvenire sia con strumenti elettronici sia in forma cartacea. I supporti elettronici di cui Duemilauno Agenzia Sociale si serve sono sia del tipo elaboratori in rete pubblica, sia del tipo elaboratori in rete privata. I supporti cartacei, ivi inclusi quelli contenenti immagini, sono ordinatamente raccolti in schedari, per essere archiviati, una volta terminato il ciclo lavorativo.

- **SEDE LEGALE**, in Muggia, Trieste, via Colombara di Vignano n. 3, in zona periferica a vocazione artigianale ed industriale. E' costituita da un edificio industriale isolato. Gli uffici si trovano al primo piano, con accesso indipendente e separato. Nei locali degli uffici si raccolgono le pratiche e gli schedari relativi alla gestione della Cooperativa (c.d. unità organizzativa "Societario"), con raccolta e trattamento di dati attinenti i soci, nonché di curricula concernenti lavoratori già in forza e potenziali altri; questo secondo archivio è accessibile solo dagli incaricati dell'UO Societario (trattasi di archivio solo cartaceo) mentre la prima banca dati è accessibile da qualsiasi incaricato della cooperativa, dietro autenticazione e password (trattasi di archivio elettronico). Sempre nella **SEDE LEGALE** si svolge il trattamento relativo alla predisposizione delle buste paga, ivi incluso il

trattamento strumentale dei dati concernenti la maternità e lo stato di malattia dei soci lavoratori; gli archivi elettronici sono gestiti da due computer situati su due scrivanie, accessibili in rete. All'UO "Amministrazione", che conta due addetti, compete di trattare i dati dei fornitori e dei clienti, per la correlata attività di fatturazione. Le fatture dei fornitori sono archiviate in schedari nonché su supporto elettronico; quelle emesse per i clienti, sono conservate solo in forma elettronica; gli elaboratori, in questo caso, rientrano nella tipologia "non accessibili da altri elaboratori o terminali". L'area è protetta da un sistema elettronico di allarme, collegato con centrale di telesorveglianza convenzionata. Il server è sistemato all'interno di un apposito mobile metallico chiuso a chiave. Al pian terreno dello stesso edificio si trova il bar/ ristorante della cooperativa Duemiladieci, che condivide gli uffici con la Duemilauno Agenzia Sociale. Gli archivi cartacei ed informatici di Duemiladieci sono separati da quelli di Duemilauno Agenzia Sociale e non accessibili. Duemiladieci ha adottato opportuno DPS e le misure minime di protezione dei dati che la riguardano.

- **PADIGLIONE M** in Trieste, via de Pastrovich n.1, in zona centrale. E' una stanza dotata di dispositivo di chiusura all'interno di un edificio dell'A.S.S. n.1 Triestina, nel comprensorio dei San Giovanni. Tratta dati provenienti da diversi servizi della Cooperativa sia in forma cartacea che informatica e non è accessibile ad utenti o estranei ai servizi. I dati cartacei vengono custoditi in armadi dotati di serratura;
- **UFFICIO DI MONFALCONE,** a Monfalcone (GO), via Pacinotti 23, in zona centrale, è una stanza dotata di dispositivo di chiusura al piano terra, tutto adibito ad uffici, di un condominio di civile abitazione. Non è di norma accessibile agli utenti dei servizi di competenza e vi vengono trattati documenti e relazioni, anche contenenti dati sensibili esclusivamente in forma cartacea. Tali documenti sono conservati in un apposito armadio dotato di serratura;
- **UFFICIO DI UDINE** in Udine, via Pozzuolo 330, in zona semiperiferica. E' una stanza dotata di dispositivo di chiusura all'interno di un edificio del comprensorio Sant'Osvaldo. Tratta dati provenienti dai servizi psichiatrici dell'Udinese, che vengono trattati sia in forma cartacea che informatica. La stanza non è accessibile agli utenti dei servizi.

La seconda macro area comprende le varie sedi operative dei servizi, quali asili, comunità residenziali e centri diurni, dove è prevista la presenza degli utenti dei servizi.

- **NIDO D'INFANZIA IL GIRASOLE,** in Frazione Stazione di Prosecco n. 28, Sgonico, in provincia di Trieste, situato in un edificio di tipo industriale di proprietà della RFI. Il nido è dotato di computer con collegamento internet ma i dati inerenti i bambini accolti vengono trattati solamente in forma cartacea e sono conservati in apposito armadio chiuso a chiave;
- **NIDO D'INFANZIA ARCOBALENO** in Sacile (PN),via Chiaradia 11,in zona periferica**.** Vengono trattati i dati dei bambini accolti in forma cartacea e gli stessi vengono conservati in armadi con serratura. I dati raccolti in forma informatica sono contenuti in computer protetto da password, in una stanza non accessibile ai bambini;
- **NIDO D'INFANZIA IL MIGNOLO,** in Gradisca di Spilimbergo (PN), via Monte Nero 9,in zona centrale. Il nido è dotato di computer con collegamento internet ma i dati inerenti i bambini accolti vengono trattati solamente in forma cartacea e vengono conservati in una stanza con serratura alla quale hanno accesso soltanto le operatrici;
- **NIDO D'INFANZIA IL FUTURO SIAMO NOI,** asilo nido aziendale del Lloyd Adriatico, in Trieste, via Maestri del Lavoro 12. in zona semicentrale. L'asilo è ricavato in un'ala degli uffici del Loyd Adriatico. Il nido è dotato di computer con collegamento internet ma i dati inerenti i bambini accolti vengono trattati solamente in forma cartacea e vengono conservati in una stanza con serratura alla quale hanno accesso soltanto le operatrici;
- **NIDO D'INFANZIA I CUCCIOLI DELLA SCIENZA – SABRINA MANCARDI**, asilo nido aziendale dell'AREA Science Park , in Trieste, località Padriciano 99. in zona periferica. L'asilo è ricavato in edificio su unico piano di proprietà dell'Area Science Park. Il nido è dotato di computer con collegamento internet ma i dati inerenti i bambini accolti vengono trattati solamente in forma cartacea e vengono conservati in una stanza con serratura alla quale hanno accesso soltanto le operatrici;
- **NIDO D'INFANZIA PRIMA DI VOLARE**, in via Barco a Pravisdomini (PN), in zona periferica**,** in un edificio isolato di proprietà del comune di Pravisdomini. Vengono trattati i dati dei bambini accolti in forma cartacea e gli stessi vengono conservati in armadi con serratura. I dati raccolti in forma informatica sono contenuti in computer protetto da password, in una stanza non accessibile ai bambini;
- **COMUNITÀ VANESSA**, in Trieste, via Machiavelli 20, in zona centrale. E' una comunità residenziale che si occupa di percorsi terapeutico - riabilitativi rivolti a piccoli nuclei famigliari in difficoltà (giovani madri e i loro figli minori di 14 anni). E' un appartamento situato in un edificio ottocentesco in cui, oltre agli spazi destinati all'abitazione degli ospiti, vi è un ufficio chiuso con dispositivo a serratura, nel quale si trova un computer opportunamente protetto da password. Il trattamento dei dati avviene sia in forma cartacea che informatizzata.
- **CENTRO DIURNO CST,** in Trieste, via Weiss, in zona centrale,in un edificio ad un piano all'interno del comprensorio di San Giovanni. I dati relativi agli utenti sono trattati solamente in forma cartacea e custoditi in armadio protetto da serratura;
- **COMUNITA' PINTURICCHIO**, in Trieste, via Pinturicchio 22, in zona semicentrale. E' una struttura residenziale con funzioni socio – riabilitative, costituita da una casetta su due piani. I dati vengono trattati in forma cartacea custoditi in apposito armadio dotato di serratura in una stanza al primo piano non accessibile agli utenti;
- **APPARTAMENTO VALDIRIVO** in Trieste,via Valdirivo 30, in zona centrale**.** E' una struttura residenziale con funzioni socio – riabilitative situata al secondo piano di un edificio d'epoca. I dati vengono trattati solo in forma

cartacea e conservati in uno stanzino dotato di dispositivo di chiusura al quale hanno accesso solamente gli operatori;

- **RESIDENZA I**, in Trieste, via De Pastrovich 2, zona centrale, in un edificio su due piani all'interno del comprensorio di San Giovanni. Si occupa di percorsi terapeutici e riabilitativi, anche con scopo residenziale; la residenza è composta di un appartamento in cui, altre agli spazi destinati all'abitazione degli ospiti, vi è un ufficio chiuso con dispositivo a serratura, nel quale si trova un archivio. Il trattamento dei dati avviene solo in forma cartacea;.
- **RESIDENZA G**, in Trieste, via De Pastrovich 2, zona centrale, in un edificio su due piani all'interno del comprensorio di San Giovanni. Si occupa di percorsi terapeutici e riabilitativi, anche con scopo residenziale; la residenza è composta di un appartamento in cui, altre agli spazi destinati all'abitazione degli ospiti, vi è un ufficio chiuso con dispositivo a serratura, nel quale si trova un archivio. Il trattamento dei dati avviene solo in forma cartacea;.
- **RESIDENZA SAN MARCO,** in Trieste, via San Marco 19, zona semicentrale. Struttura residenziale terapeutico – riabilitativa, consta di un appartamento sito al primo piano di un edificio adibito ad abitazioni private. Vi hanno accesso gli operatori, gli ospiti, i familiari. I dati sono trattati solo in forma cartacea e sono conservati in apposito armadio munito di serratura;
- **RESIDENZA Z** in Trieste, via Weiss 16, zona centrale, costituito da una casetta ad un piano fuori terra isolata, all'interno del comprensorio di San Giovanni**.** Struttura con finalità assistenziali e di fornitura di residenza, con personale operatore sempre presente, visite di familiari e colloqui con i pazienti utenti. I dati sono trattati solo in forma cartacea e sono custoditi in apposita cassaforte presente nella residenza;
- **VILLA PRIMAVERA** in Udine, via Pozzuolo 330, in zona semiperiferica. E' una struttura residenziale che si occupa di percorsi terapeutici e tratta i dati della persona che viene accolta e dei parenti di questa. E' costituito da un edificio isolato a due piani all'interno del comprensorio di Sant'Osvaldo. I dati personali vengono trattati sia in forma informatica che cartacea. Il computer è protetto da opportuna password, mentre la documentazione cartacea viene conservata in un armadio dotato di serratura.
- **RESIDENZA DI VIA MARANGONI** in Udine, via Marangoni 105, in zona centrale**,**in un edificio di proprietà dei padri missionari vicenziani. Offre domicilio ed assistenza agli ospiti, acquisendo da questi le informazioni necessarie per i percorsi riabilitativi. I dati personali vengono trattati sia in forma informatica che cartacea. Il computer è protetto da opportuna password, mentre la documentazione cartacea viene conservata in un armadio dotato di serratura.
- **RESIDENZA DI VIALE VOLONTARI DELLA LIBERTA',** in Udine, viale Volontari della Libertà 34, in zona centrale. Costituita da due piccoli appartamenti contigui di proprietà dell'azienda sanitaria locale, è una residenza con funzioni terapeutico – riabilitative per adulti. I dati personali vengono trattati sia in forma informatica che cartacea. Il computer è protetto da opportuna password, mentre la documentazione cartacea viene conservata in un armadio dotato di serratura. Gli operatori della cooperativa sono presenti in orario diurno, fino alle ore 21.00;
- **RESIDENZA MANZANO,** in Manzano (UD), via Drusin 25, in zona semicentrale. Residenza con funzioni terapeutico - riabilitative composta da 6 appartamenti duplex a schiera, ciascuno per tre ospiti. L'ambiente in cui sono custoditi i dati cartacei ed elettronici, centrale rispetto alla schiera di appartamenti, vede la presenza quasi costante di almeno un operatore: nei momenti in cui questi è assente, la stanza è chiusa a chiave;
- **RESIDENZA PAGNACCO,** in Pagnacco (UD), piazza Libertà 11, in zona centrale. Offre domicilio ed assistenza agli ospiti. L'appartamento è composto di dieci locali, ricavati dall'unione di due appartamenti all'interno di un complesso residenziale. I dati sono trattati sia in forma cartacea che informatica nella cosi detta sala operativa, dotata di armadietto con lucchetto, armadio, computer dotato di password;
- **RESIDENZA DI VIA DI GIUSTO,** in Udine, via di Giusto 82, in zona centrale, al primo piano di una palazzina residenziale. La residenza si occupa di percorsi di integrazione sociale, trattando dati relativi agli ospiti ed elabora progetti di riabilitazione individuale. Vi è continua sorveglianza da parte degli operatori. I dati sono conservati in armadi chiusi a chiave e le chiavi sono in possesso soltanto degli operatori. I dati trattati con l'ausilio del PC sono protetti da password;
- **COMUNITA' IL MULINO,** in Aquilieia (UD),via della Stazione 8, in zona centrale, in un edificio su due piani con ingresso autonomo. E' una comunità con scopi socio riabilitativi per minori. I dati sono trattati sia in forma cartacea che elettronica e le attrezzature sono protette da password e dislocate in una stanza accessibile solo agli operatori;

1.3 La mappa dei trattamenti effettuati

In relazione al diverso grado di rischio, è opportuno distinguere i trattamenti che vengono posti in essere nelle distinte aree in cui sono dislocati gli strumenti. Il simbolo X, apposto nella casella di incrocio, significa che determinati tipi di dati sono trattati con determinati strumenti:

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a clienti / utenti / consumatori	X	X	X	X	X
2 - Dati comuni relativi a fornitori	X		X		X
3 - Dati comuni relativi ad altri soggetti	X		X		X
4 – Dati relativi ai soci ed ai dipendenti……	X		X		X
5 - Dati di natura anche sensibile relativi a clienti / utenti	X	X	X	X	
6- Dati idonei a rivelare lo stato di salute e/o la vita sessuale di clienti/utenti		X		X	
7 - Dati idonei a rivelare l'affezione da virus HIV		X		X	
	AA	**AB**	**BA**	**BB**	**C**

STRUMENTI UTILIZZATI

Legenda degli strumenti utilizzati per il trattamento:
A – Schedari ed altri supporti cartacei, nell'ambito dei quali si procede a suddividere:
- **AA** quelli custoditi nella sede legale
- **AB** quelli custoditi presso le altre unità operative

B – Elaboratori non in rete, nell'ambito dei quali si procede a suddividere:
- **BA** quelli localizzati nella sede legale
- **BB** quelli localizzati presso le altre unità operative

C – Elaboratori in rete pubblica presso la sede legale ed alcune delle unità operative esterne ad essa

Da una prima lettura della mappa, si può considerare che la logica del trattamento obbedisce ad adeguati parametri di sicurezza; in fatti, i dati vengono trattati solo dai soggetti che abbiano necessità di conoscerli e vengono poi cancellati, nel momento in cui detto trattamento non sia più necessario: i dati comuni relativi a fornitori, pazienti utenti, familiari etc… vengono gestiti con analoghe modalità di sicurezza mentre le informazioni sensibili concernenti lo stato di salute, la vita sessuale e l'infezione da HIV, la cui conoscenza è strumentale ai trattamenti terapeutici posti in essere, sono a conoscenza dei soli soggetti cui l'informazione possa risultare utile per i fini medesimi.

2. Mansionario privacy ed interventi formativi degli incaricati

Per il trattamento dei dati personali, il Titolare ha nominato come responsabile del trattamento dati il sig Fabio Vallon

Il trattamento dei dati personali viene effettuato solo da **soggetti che hanno ricevuto un formale incarico**, mediante documentata preposizione di ogni persona ad un'unità, per la quale sia stato previamente individuato per iscritto l'ambito del trattamento, consentito agli addetti all'unità medesima

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ad ogni aspetto della gestione della riservatezza dei dati, per esempio: procedure da seguire per la classificazione dei dati, 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; 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.

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.

Nel seguente schema si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- sull'asse verticale si riportano i dati personali oggetto di trattamento, quali emergono dall'analisi effettuata del presente documento
- sull'asse orizzontale si riportano le unità organizzative in cui si suddivide l'organizzazione del Titolare
- l'apposizione del simbolo x, in corrispondenza della casella di intersezione tra le due coordinate, significa che una determinata unità organizzativa procede al trattamento dei dati indicati nelle righe:

TIPI DI DATI TRATTATI

1 - Dati comuni relativi a utenti				X
2 - Dati comuni relativi a fornitori		X		
3 - Dati comuni relativi ai soci ,ai lavoratori nonché ai candidati per diventarlo	X		X	
4 - Dati comuni relativi ai committenti		X		
5 - Dati di natura anche sensibile relativi a utenti – compreso il dato di infezione da HIV				X
	A	**B**	**C**	**D**
	UNITA' ORGANIZZATIVE			

La legenda delle unità organizzative è la seguente:
A – ufficio societario
B – amministrazione
C – ufficio paghe
D – unità operative periferiche

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 già al momento dell'ingresso in servizio ed in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali; la formazione è anche pensata in funzione dell'eventuale introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno sia all'esterno, presso soggetti specializzati.

3. Analisi dei rischi che incombono sui dati

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono
- quelli legati alle caratteristiche degli strumenti utilizzati per procedere al trattamento dei dati.

Si stima il grado di rischio, che dipende dalla **tipologia dei dati trattati dal Titolare**, combinando il fattore della loro appetibilità per i terzi, con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono:

	ELVATISSIMO				
GRADO DI INTERESSE PER I TERZI	**ALTO**			Dati sensibili di pazienti utenti, dati su infezione da HIV	
	MEDIO				
	BASSO	Dati comuni di clienti, fornitori e di altri soggetti	Dati comuni relativi a dipendenti e potenziali dipendenti		
		BASSO	**MEDIO**	**ALTO**	**ELEVATISSIMO**

PERICOLOSITA' PER LA PRIVACY DELL'INTERESSATO

Per quanto concerne gli **strumenti impiegati per il trattamento**, le componenti di rischio possono essere idealmente suddivise in:

1. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti)
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici)
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti)
3. rischio di penetrazione logica nelle reti di comunicazione
4. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti.

Nella tabella che segue si evidenziano i fattori di rischio cui sono soggette le unità organizzative attraverso le quali cui l'organizzazione procede al trattamento dei dati personali. Il simbolo x, posto nella casella di intersezione, significa che l'esposizione al rischio è modesta; il simbolo y significa che l'esposizione al rischio è elevata; la mancanza di indicazione attesta che il rischio è tendenzialmente assente.
Nell'elaborare la tabella, si è tenuto conto anche di alcuni fattori legati alla struttura del Titolare, nei seguenti termini:
il rischio d'area, legato alla eventualità che persone non autorizzate possano accedere nei locali in cui si svolge il trattamento, è giudicato basso o tendenzialmente assente in funzione della struttura della sede legale, per i dati trattati in tale contesto; è anche giudicato basso per le unità periferiche, in considerazione del fatto che in queste sono sempre presenti gli operatori.
Il rischio di guasti tecnici delle apparecchiature interessa i soli strumenti elettronici: in tale contesto, è giudicata più rischiosa la situazione degli strumenti non in rete che, essendo affidati a singoli che non sempre possiedono un bagaglio tecnico adeguato, presentano un rischio di rottura maggiore, rispetto agli impianti che vengono gestiti da persone con specifiche competenze.
Il rischio di penetrazione logica nelle reti di comunicazione interessa, essenzialmente, i soli strumenti che sono tra loro collegati tramite una rete di comunicazione accessibile al pubblico.
Il rischio legato ad atti di sabotaggio, o ad errori umani delle persone, presente in tutte le tipologie di strumenti utilizzati, è maggiore per quelli che sono in rete.

Tipologia di rischio				
Rischio d'area, legato al verificarsi di eventi distruttivi				X
Rischio d'area, legato all'accesso non autorizzato nei locali	X	X	X	X
Rischio di guasti tecnici di hardware, software e supporti	X	X	X	
Rischio di penetrazione logica nelle reti di comunicazione	X	X	X	
Rischio legato ad atti di sabotaggio e ad errori umani	X	X	X	X
	A	**B**	**C**	**D**

Unità organizzative

La legenda delle unità organizzative è la seguente:
A – societario
B – amministrazione
C – paghe
D – unità operative periferiche

4. Misure atte a garantire l'integrità e la disponibilità dei dati

Nel presente paragrafo vengono descritte le misure atte a garantire:
- la protezione delle aree e dei locali, nei quali 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 dell'utilizzo degli strumenti elettronici.

Si procede alla descrizione:
- delle misure che risultano già adottate dal Titolare, nel momento in cui viene redatto il presente documento
- delle ulteriori misure, finalizzate ad incrementare la sicurezza nel trattamento dei dati, la cui adozione è stata programmata, anche per adeguarsi alle novità introdotte dal Dlgs 196/2003, e dal disciplinare tecnico in materia di misure minime di sicurezza, allegato a tale decreto sub b).

4.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti da dispositivi antincendio.
Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si svolge il trattamento sono protetti dalla presenza degli operatori e da adeguati sistemi di chiusura a serratura, oltre che dalla presenza di schedari, e armadi chiusi a chiave.

4.2 La diffusione dei sistemi informatici e la loro protezione

Nel corso del 2008 si è continuato a dotare tutte le strutture di strumenti informatici adeguatamente protetti, anche avvalendosi di contributi pubblici. Sono stati inoltre acquistati diversi notebook.
Nella sede legale nel corso del 2008 si provvede a verificare costantemente le attrezzature esistenti e si è provveduto ad acquistare un nuovo server e nuove attrezzature elettroniche. E' stata installata una ulteriore protezione fisica del server centrale ì con opportuno armadio/rack metallico.
La sede legale della cooperativa è stata inoltre dotata di sistema di allarme antintrusione collegato con una centrale di telesorveglianza convenzionata. L'allarme viene inserito al termine della giornata lavorativa da personale opportunamente addestrato e disattivato al mattino in concomitanza all'apertura del sottostante bar (entro le ore 07.00 dal lunedì al venerdì). Il centro di telesorveglianza convenzionato dispone di alcuni cellulari di pronta reperibilità del personale della cooperativa in caso di necessità.

Si proseguirà, anche durante il 2009 con i necessari interventi di manutenzione degli impianti e dei sistemi operativi, sia per garantire il necessario livello di operatività sia le opportune misure di sicurezza relativamente al trattamento di dati personali.

4.3 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, fotografie, pellicole….), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o ad un responsabile del trattamento, o direttamente al titolare.

Di conseguenza, agli incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

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: 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 con serratura ed armadi chiudibili a chiave, nei quali devono riporre i documenti, contenti dati sensibili, 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.
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.

Gli archivi contenenti dati sensibili o giudiziari sono controllati, mediante l'adozione dei seguenti accorgimenti: ad alcune persone, aventi la scrivania prospiciente, viene dato l'incarico di vigilare gli archivi, dettando precise istruzioni in merito al fatto che una persona deve essere sempre presente, durante l'orario di apertura dell'archivio, per controllare chi vi accede; agli operatori delle unità operative periferiche viene dato incarico di vigilare costantemente sugli archivi presenti.

Gli impianti e le attrezzature, di cui è dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari appaiono soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti. Per l'anno 2006, sono quindi previsti semplicemente interventi di manutenzione e di rimpiazzo

4.4 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone, affinché ad ogni strumento elettronico possa accedere solo chi è autorizzato
- realizzazione e gestione di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

Il **sistema di autenticazione informatica** viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle **credenziali di autenticazione** per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione 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.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- dovere di custodire i dispositivi, attribuiti agli incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici: la custodia deve avvenire in modo diligente,
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa, nonché sulle altre componenti riservate della credenziale di autenticazione (username),. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili.

Le password sono composte da almeno otto caratteri.

Agli incaricati è prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:

- 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
- 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. 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.

Per quanto concerne le **tipologie di dati ai quali gli incaricati possono accedere**, ed i trattamenti che possono effettuare, si osserva che si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.
Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e dal responsabile, ovvero da soggetti da questi appositamente incaricati. Il profilo di autorizzazione non viene in genere studiato per ogni singolo incaricato, ma è generalmente impostato per classi omogenee di incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale). L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun incaricato o di ciascuna classe omogenea di incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Per quanto riguarda la **protezione, di strumenti e dati**, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi 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 (comunemente conosciuti come virus).
A tale fine, si è dotati di idonei strumenti elettronici e programmi che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- ogni 3 mesi nel caso di strumenti elettronici in rete pubblica
- ogni 6 mesi nel caso di strumenti elettronici in rete privata
- ogni anno nel caso di strumenti elettronici che non sono in rete.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall, che il nuovo codice privacy ha reso obbligatoria per i casi in cui si trattino dati sensibili o giudiziari.
A tale riguardo il Titolare si è da tempo dotata di tali strumenti, per la protezione degli elaboratori in rete

Per quanto concerne i **supporti rimovibili** (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, la norma impone particolari cautele solo nell'ipotesi in cui essi contengano dati sensibili. La nostra organizzazione ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati. Per l'anno 2006, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento, alla manutenzione, ed a qualche rimpiazzo.

5. Criteri e modalità di ripristino dei dati

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per i dati sensibili e giudiziari.
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 conservati nel data base del server situato presso gli uffici della sede legale avviene come segue:

- in maniera automatica con procedura di backup interno con frequenza giornaliera (lunedì, martedì, mercoledì, giovedì, venerdì);
- attraverso un'unità di backup esterna, a cura del Responsabile del trattamento, con frequenza settimanale. L'unità di backup esterna è custodita dal Responsabile del trattamento in luogo esterno alla sede legale;

Per dati trattati con strumenti elettronici non collegati al server, sono previste procedure di salvataggio consistenti nella duplicazione settimanale dei dati su supporti removibili adeguatamente protetti e conservati dagli incaricati.

6. Controllo generale dello stato della sicurezza

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. Verifica inoltre l'efficacia delle misure adottate relativamente a:

- accesso fisico ai locali dove si svolgono i trattamenti
- procedure di archiviazione e custodia dei dati trattati
- efficacia e utilizzo delle misure di sicurezza degli strumenti elettronici
- integrità dei dati e delle loro copie di backup
- distruzione dei supporti magnetici non più utilizzabili
- livello di informazione degli interessati

7. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel marzo del 2009, viene firmato in calce da:

- Stefano GARBELLOTTO, in qualità di Presidente del Consiglio di Amministrazione e rappresentante legale del Titolare;
- Fabio VALLON, in qualità di responsabile del trattamento dati.

Esso verrà sottoposto per l'approvazione al Consiglio di Amministrazione, e successivamente trascritto nel libro sociale che riporta le delibere prese dallo stesso.

Il presente documento viene pubblicato sul sito web della cooperativa, accessibile nell'area riservata ai soci. Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali (ad esempio, nel caso in cui dovessero essere nominati responsabili per determinati trattamenti di dati personali).
L'originale viene custodito presso la sede della società, per essere esibito in caso di controlli.

Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento, che costituisce la terza redazione del Documento Programmatico sulla Sicurezza

Muggia, 23 marzo 2009

Firma del rappresentante legale del Titolare…… 

Firma del responsabile del trattamento dati……