Documento Programmatico sulla Sicurezza

Indice

1. Finalità del documento

La Insieme si può Soc. Coop. Soc.-, di seguito denominata Cooperativa, tratta dati personali sensibili.

Il presente Documento Programmatico sulla Sicurezza è redatto, ai sensi degli articoli 33 e seguenti del Dlgs 196/2003 e secondo le previsioni dell'Allegato B a tale decreto , per definire e descrivere le politiche di sicurezza adottate dalla Cooperativa in materia di trattamento di dati personali ed i criteri organizzativi seguiti per la loro attuazione e per fornire idonee informazioni a riguardo anche di parti terze.

2. Inventario dei beni della Cooperativa da proteggere

Le informazioni fornite di seguito sono state valutate come utile supporto per fornire informazioni idonee a valutare la politica di sicurezza perseguita dalla Cooperativa.

La Cooperativa ha sede in Milis, nella Via Grazia Deledda n. 2. Alla data di redazione del presente documento lavorano e collaborano nella Cooperativa n. 130 PERSONE di cui n.15 dipendenti.

La Cooperativa non è dotata di un sistema informatico proprio, ma usufruisce dell'ospitalità della Fondazione Istituti di Assistenza Sociale- Onlus, sita in Milis nella via G.Brotzu n.6, che si è dotata di un sistema di protezione informatica così come richiesto dalle linee guida del Dlgs n.196/03. per la sede di Sestu invece usufruisce dell'ospitalità di Gersia soggetto affidatario , sita in Selargius, vi della Libertà 84, che si è dotata di un sistema di protezione informatica così come richiesto dalle linee guida del Dlgs n.196/03

Il trattamento dei dati avviene sia attraverso strumenti elettronici sia attraverso strumenti diversi.

3. Elenco dei trattamenti di dati personali gestiti nella Cooperativa

Sono stati individuati i seguenti trattamenti riepilogati in tabella:

Categoria Dati soggetti a trattamento e Soggetti a cui si riferiscono (ai sensi dell'art. 4 D.Lgs 196/2003 c. 1 lettera a)	**Finalità del trattamento**	**Modalità di trattamento**	**Luogo di custodia dei dati**
Archivi dati contabili riferiti a clienti fornitori	Tenuta della contabilità e gestione adempimenti fiscali e civili correlati	Il trattamento è svolto mediante software ad hoc di gestione della contabilità	I dati sono custoditi sulle seguenti macchine hardware: **Server Fondazione** I libri obbligatori per legge e le pezze di appoggio cartacei sono tenute nell'archivio dell'ufficio messo a disposizione dalla F.I.R.A.S.
Archivi dati personali dipendenti, varie tipologie collaboratori.	Gestione ordinaria attività con tali controparti	Gli archivi sono sia in formato elettronico che cartaceo	I dati sono custoditi sulle seguenti macchine hardware **Server Fondazione** I libri obbligatori per legge e le pezze di appoggio cartacei sono tenute nell'archivio dell'ufficio messo a disposizione dalla F.I.R.A.S.
Archivi dichiarazioni, altri dati fiscali e contributivi	Gestione degli adempimenti fiscali obbligatori	Il trattamento è svolto mediante software ad hoc di gestione delle dichiarazioni ;	I dati sono custoditi sulle seguenti macchine hardware **Server Fondazione** I libri obbligatori per legge e le pezze di appoggio cartacei sono tenute nell'archivio dell'ufficio messo a disposizione dalla F.I.R.A.S.
Archivi dati bilancio e dati correlati (ad esempio elenco soci)	Gestione adempimenti civilistici inerenti il bilancio di società clienti	Il trattamento è svolto mediante software ad hoc Gli archivi sono sia in formato elettronico che cartaceo	I dati sono custoditi sulle seguenti macchine hardware **Server Fondazione** I libri obbligatori per legge e le pezze di appoggio cartacei sono tenute nell'archivio dell'ufficio messo a disposizione dalla F.I.R.A.S.
Archivi dati amministrativi Utenti.	Gestione adempimenti amministrativi inerenti la fatturazione verso il Commitente, l'elaborazione di dati a fini di statistica	Il trattamento è svolto mediante software ad hoc Gli archivi sono sia in formato elettronico che cartaceo	I dati sono custoditi sulle seguenti macchine hardware **Server Fondazione** I libri obbligatori per legge e le pezze di appoggio cartacei sono

Categoria Dati soggetti a trattamento e Soggetti a cui si riferiscono (ai sensi dell'art. 4 D.Lgs 196/2003 c. 1 lettera a)	Finalità del trattamento	Modalità di trattamento	Luogo di custodia dei dati
			tenute nell'archivio dell'ufficio messo a disposizione dalla F.I.R.A.S.

4. Distribuzione dei compiti e delle responsabilità nell'ambito del personale preposto al trattamento dei dati

La Sig.ra Tola Rita Erina è stata nominata in data 01.03.2007 RESPONSABILE DEL TRATTAMENTO a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate nel documento di nomina allegato e in questo documento programmatico sulla sicurezza.

Si è valutato che la Sig.ra Tola Rita Erina sia in possesso dei requisiti di esperienza, capacità ed affidabilità richiesti dal comma 2 dell' art. 29 del Dlgs 196/2003.

I signori:

Nome e Cognome	Codice fiscale
Pitzus Miranda	PTZMND65S67F208I
Manca Simonetta	MNCSNT66L48L219X
Enna Maria Sofia	NNEMSF72L61F208Z
Sanna Francesco	SNNFNC73P10G113H
Carboni Graziella	CRBGZL77E70G113N
Fanari Agnese	FNRGNS74C63F208Q
Manca Annamaria	MNCNMR72E58B354C
Crobe Elisabetta Caterina	CRBLBT74C51F208I
Mastinu Antonella	MSTNNL70H49F208A
Cesare Desogus	DSGCSR63H24F979P
Pronesti Domenico	PRN DNC 68A27 H558W
Manuela Serra	SRRMNL70P43B354Q
Paola Putzolu	PTZPLA81R65G113V

sono stati nominati INCARICATI DEL TRATTAMENTO.

In questo ruolo e nei limiti delle mansioni a Loro affidate, tali soggetti potranno eseguire le operazioni di trattamento riguardanti le sopraddette banche dati, attenendosi alle istruzioni impartite dal titolare o dal responsabile del trattamento.

Nel singolo documento di nomina allegato, sono evidenziate le operazioni riguardanti il trattamento di dati personali di propria competenza e le banche dati a cui il singolo incaricato può accedere.

5. Analisi sintetica dei rischi che incombono sui dati:

Ad un livello generale sono state individuate le seguenti principali minacce alla sicurezza dei dati gestiti suddivise in tre macrocategorie:

Calamità naturali	Minacce intenzionali	Minacce involontarie
• Incendio • Fulmine • Inondazione	• Accessi non autorizzati • Virus informatici • Furto di dati e di attrezzature hardware	• Black out elettrico • Malfunzionamenti nel software • Malfunzionamenti hardware • Errori umani nell'utilizzo del sistema informatico

In riferimento alla sicurezza dei dati personali gestiti, la Cooperativa pone i seguenti obbiettivi:

Obiettivo:	Cosa significa:
Riservatezza	I DATI DEVONO ESSERE ACCESSIBILI SOLO ALLE PERSONE AUTORIZZATE
Integrità	I DATI DEVONO ESSERE PROTETTI DA MODIFICAZIONI E DANNEGGIAMENTI
Disponibilità	I DATI DEVONO ESSERE ACCESSIBILI ALLE PERSONE AUTORIZZATE

Attraverso l'implementazione di una serie di misure di sicurezza, esposte in dettaglio nei successivi paragrafi, si vuole ridurre le vulnerabilità del sistema informativo della Cooperativa, raggiungendo un livello di rischio valutato accettabile.

In sintesi :

Tutelare l'obiettivo:	Significa:
Riservatezza	Ridurre il rischio che persone non autorizzate possano accedere alle informazioni
Integrità	Ridurre il rischio che le informazioni siano non volutamente modificate o cancellate
Disponibilità	Ridurre il rischio di non poter accedere anche se autorizzati alle informazioni

6. Misure di sicurezza adottate:

6.1 Protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità:

Gli ingressi dei locali dove sono custoditi i dati sono protetti da porte, alcune delle quali anche blindate; le finestre sono protette da tapparelle particolarmente robuste e le camere sono dotate anche di un sistema di allarme anti intrusione**.**

L'accesso fisico alle stanze contenenti documenti trattanti dati personali è permesso solo agli incaricati del trattamento.

Alcuni armadi in cui sono conservati documenti cartacei inerenti dati personali sono dotati di serratura a chiave.

6.2 Gestione strumenti cartacei all'interno dei reparti.

La gestione delle cartelle personali e dei documenti contenenti dati sensibili relative agli utenti del S.A.D.,e' disciplinata da apposita procedura redatta dal RQ – Paola Putzolu

6.3 Gestione strumenti elettronici:

Back up dati

Al fine di garantire non solo l'integrità, ma anche la pronta disponibilità dei dati la F.I.R.A.S. è dotata di strumenti e procedure di back up, che garantiscono alla Cooperativa una corretta conservazione e protezione dei dati sensibili trattati..

Tutti i dati personali gestiti con strumenti elettronici vengono inclusi nella procedura di backup.

Le procedure di back up avvengono nel seguente modo:

6.4 Hard disk esterno:

- Con cadenza **settimanal**e ad opera del responsabile del trattamento della F.I.R.A.S. vengono salvati i seguenti dati:
- dati relativi all'archivio pazienti;
- dati relativi alla gestione contabile e amministrativa;
- dati relativi alla gestione del personale;
- cartella dati condivisi dagli utenti;
- dati relativi alla rilevazione presenze;
- dati relativi alle cartelle neonati;
- sottocartelle di lavoro.

6.5 Disco esterno PC qualita':

Periodico salvataggio dei dati di lavoro , della Cartella Qualità e del software Atlante.

I dati personali trattati sono gestiti sui seguenti strumenti elettronici connessi in rete:

6.6 Locale archivio

- **n. 1 server Athena** dotato di doppio alimentatore, n. 2 dischi fissi da 18 GB estraibili a caldo, doppia ventilazione;
- **n. 1 Pc** dedicato principalmente alla lettura dei dati del centralino e al passaggio degli stessi sulla procedura gestionale dei clienti.

6.7 Locale direzione amministrativa

- **n. 1 PC Asus** dotato di hard disk esterno
- **n. 1 PC Philips** dotato di hard disk esterno

Il Dott. Cesare Desogus è incaricato di gestire le copie di sicurezza e le procedure di backup.

In caso di assenza del Dott. Cesare Desogus, la sig.ra Daniela Solinas si occuperà della procedura di backup.

Le copie di back up vengono custodite nella cassaforte della Fondazione.

Il tempo massimo per la conservazione delle copie di back up è stato stabilito in 10 anni.

I supporti da eliminare vengono resi inutilizzabili dal signor Dott. Cesare Desogus.

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo, comunque ampiamente sotto il limite dei sette giorni previsti dal punto 23 dell'allegato B del D.Lgs. 196/2003 in ipotesi di trattamento di dati sensibili.

Antivirus

La Cooperativa si è dotata del software antivirus **Norton Antivirus 2003.**

L'aggiornamento del prodotto antivirus istallato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.

L'antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali floppy disk e cd rom.

Il personale è stato adeguatamente informato sui comportamenti corretti da tenere per evitare di introdurre virus informatici nella rete della F.I.R.A.S.

Il responsabile del trattamento si fa carico di seguire il corretto e frequente aggiornamento del sistema operativo e dei seguenti altri software utilizzati correntemente nella F.I.R.A.S..

Gruppo di continuità

La F.I.R.A.S. è dotata di gruppo di continuità per prevenire le conseguenze dei blackout elettrici o dei picchi di sovra o sotto tensione elettrica

Il gruppo di continuità in oggetto è in grado di filtrare l'alimentazione elettrica da eventuali impurità .

Firewall e sistemi di anti intrusione

La F.I.R.A.S., come gia' detto, e' connessa alla rete internet tramite isdn fornita da TelecomItalia; il contratto prevede inoltre la protezione dall'esterno con sistema firewall.

Il firewall è stato configurato dalla società Telecom specializzata in sicurezza informatica.

Gestione manutenzione strumenti elettronici:

La manutenzione degli strumenti elettronici sia a livello hardware sia a livello software viene affidata alla ditta Microsystem di Savarese Gianfranco con contratto stipulato dalla F.I.R.A.S..

In ogni caso non sono stati resi possibili interventi di manutenzione a livello software effettuati via rete a distanza.

Sistema di identificazione e autenticazione

La F.I.R.A.S. ha attivato ed è correntemente funzionante un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.

E' stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici(di solito personal computer) del sistema informatico. I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati.

Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) a livello di sistema operativo.
Il responsabile del trattamento è incaricato della gestione delle password.
Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso.
Viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 6 mesi.
Nell'ipotesi di trattamento di dati sensibili viene segnalato ad ogni incaricato la necessità di cambiare la password almeno ogni 3 mesi
Sono normalmente vietate credenziali di autenticazione (username e password) condivise fra più persone in F.I.R.A.S.
Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate.
Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza.
Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password.
In caso di prolungata assenza dell'incaricato, il responsabile del trattamento è autorizzato ad rivelare la password in uso per assicurare la disponibilità dei dati e degli strumenti elettronici.
La visualizzazione della password sullo schermo dei personal computer e' impedita da tutti i software in uso.

Business continuity plan e disaster recovery plan

In conseguenza della limitata dimensione e della bassa complessità della struttura della cOOPERATIVA non si valuta necessario procedere all'elaborazione formale di tali documenti.
Si valuta che le misure di sicurezza attualmente implementate e gestite, esplicitate in questo documento, siano sufficienti per poter ripristinare l'attività della Cooperativa in tempi brevi e a costi contenuti al verificarsi di emergenze o di eventi negativi.

Trattamenti di dati personali affidati all'esterno della Cooeprativa

Nell'ipotesi vi fosse necessità di affidare trattamenti di dati personali all'esterno, per esempio ad altri professionisti, va richiesta a tali soggetti una dichiarazione scritta in cui viene certificata la conformità del loro sistema informativo alle previsioni della normativa sulla privacy.

Trattamenti senza l'ausilio di strumenti elettronici

Nella procedura PO- gestione dei documenti e nel modulo Registrazioni della qualità, sono impartite agli incaricati istruzioni scritte, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi contenenti gli archivi contenenti dati sensibili sono identificate e registrate.
Il responsabile del trattamento è incaricato della gestione delle autorizzazioni nei luoghi contenenti archivi di dati sensibili.

6.8 Formazione

La Cooperativa riconosce l'importanza della formazione dei suoi componenti riguardo le tematiche della sicurezza, come elemento significativo di riduzione dei rischi al proprio sistema informativo e s'impegna a promuovere momenti formativi, in particolare al momento dell'ingresso in servizio o al momento di cambiamenti di mansioni di tali soggetti o all'introduzione di nuovi strumenti elettronici che hanno impatto sul trattamento dei dati personali.

7. Modalità aggiornamento del documento programmatico per la sicurezza

Il responsabile del trattamento è il soggetto preposto all'aggiornamento e alla custodia del documento programmatico per la sicurezza.
Il documento in oggetto non deve rimanere statico ma deve essere aggiornato ogni volta che vi siano cambiamenti significativi nella Cooperativa impattanti sulle misure minime di sicurezza.
In ogni caso ogni anno entro il 31 marzo di ogni anno, il responsabile del trattamento dovrà procedere alla completa revisione del documento in oggetto.

Milis 15.03.2013

Il Responsabile del Trattamento
Rita Erina Tola