GESTIONE DATI PERSONALI E SENSIBILI TRAMITE LA PROCEDURA DENOMINATA "Sistema Informativo Fratres"

PREMESSO CHE

i donatori e le altre tipologie di soci previste dallo Statuto dei Gruppi Fratres, sono associati ad ogni singolo Gruppo tramite presentazione di una specifica domanda di iscrizione, all'atto della quale, il Presidente del Gruppo è tenuto ad informare il richiedente sulla gestione dei propri dati personali che il Gruppo deterrà ed ottenere quindi il consenso al trattamento di tali dati,

PRECISIAMO CHE

tutti i dati gestiti tramite la procedura denominata "Sistema Informativo Fratres", seppure confluenti in unico ambiente, sono tutelati con precise modalità che rispettano tutte le caratteristiche di sicurezza, poiché il trattamento dei dati dei soci è accessibile solo al Presidente del Gruppo FRATRES di loro iscrizione, in veste di Responsabile del trattamento, il quale può delegare persone (incaricati) di sua fiducia mediante specifiche autorizzazioni che peraltro sono già previste nel D.P.S. (non più obbligatorio ma consigliabile in quanto riassume tutte le necessità del caso). Dal punto di vista della sicurezza del summenzionato ambiente, il collegamento avviene con protocollo di crittografia SSL appositamente **certificato**, in sovrapposizione al normale protocollo di trasferimento ipertestuale (HTTP).

HTTPS viene utilizzato per gestire informazioni sensibili
per le quali è importante garantire un elevato livello di riservatezza ed una garanzia di integrità.

Per Vostra tranquillità l'ambiente di gestione possiede la sicurezza prevista dalla Legge sulla Privacy (cosa che comunque deve avvenire anche se i dati sono gestiti in maniera cartacea o attraverso sistemi informatici "non in rete") ed il sistema di accesso permette di soddisfare le disposizioni per le quali, il Responsabile è obbligato, in base all'art. 34 del D.Lgs. 196/2003 ad adottare particolari misure che riguardano prevalentemente le modalità di accesso, sì da poter verificare, in caso di illeciti connessi all'utilizzo dello strumento informatico, l'identità dell'autore dell'illecito o quantomeno il Responsabile dell'accesso abusivo dall'esterno. Dal livello interno ogni transazione viene registrata con riferimento all'utente che ha effettuato, l'operazione, così da tenerne traccia. Pertanto, in base al citato art. 34, mediante la gestione delle autenticazioni per l'accesso alla procedura "Sistema Informativo Fratres" sono state adottate le seguenti misure necessarie:

a) SISTEMA DI AUTENTICAZIONE INFORMATICA

Questo sistema, è oggetto di specificazione secondo le previsioni dell'allegato B, che lo richiede come requisito per poter lecitamente effettuare il trattamento di dati con strumenti informatici in rete.

Il codice di autenticazione per il primo accesso è fornito direttamente dalla Consociazione Nazionale al Presidente in carica a mezzo posta prioritaria, sulla base del modello di segnalazione dati che deve pervenire dal singolo Gruppo ad ogni variazione dell'organico del Consiglio Direttivo.

La stessa Consociazione provvede a disattivare in via permanente il codice di autenticazione del Presidente che non risulta più in carica.

In particolare, oltre al Responsabile, è consentito l'accesso ai sistemi informatici soltanto ad incaricati che siano dotati di credenziali per l'autenticazione in funzione di procedure relative ad uno specifico trattamento o ad un insieme di trattamenti.

Le credenziali di autenticazione (login), in particolare, consistono in un codice per l'identificazione dell'incaricato (user-id) associato a una parola chiave riservata (password) conosciuta solamente dal medesimo, che in maniera obbligatoria deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi. **In caso di trattamento di dati sensibili la parola chiave è obbligatoriamente modificata almeno ogni tre mesi.**

Da parte del Responsabile, ad ogni incaricato, possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione. Agli incaricati devono essere fornite dal Responsabile, oltre le istruzioni per l'autenticazione, anche le prescrizioni in merito all'adozione delle necessarie cautele per assicurare la segretezza della password nonché le istruzioni per non lasciare incustodito e accessibile lo strumento informatico durante una sessione di trattamento;

b) SISTEMA DI AUTORIZZAZIONE

Nel sistema sono individuati profili di autorizzazione di ambito diverso, corrispondenti alle cariche previste nello Statuto dei Gruppi Fratres, aventi diversi livelli di accesso, quali il Presidente ed il Capogruppo dotati di determinati privilegi, oppure profili più limitativi come il Segretario e l'Amministratore;

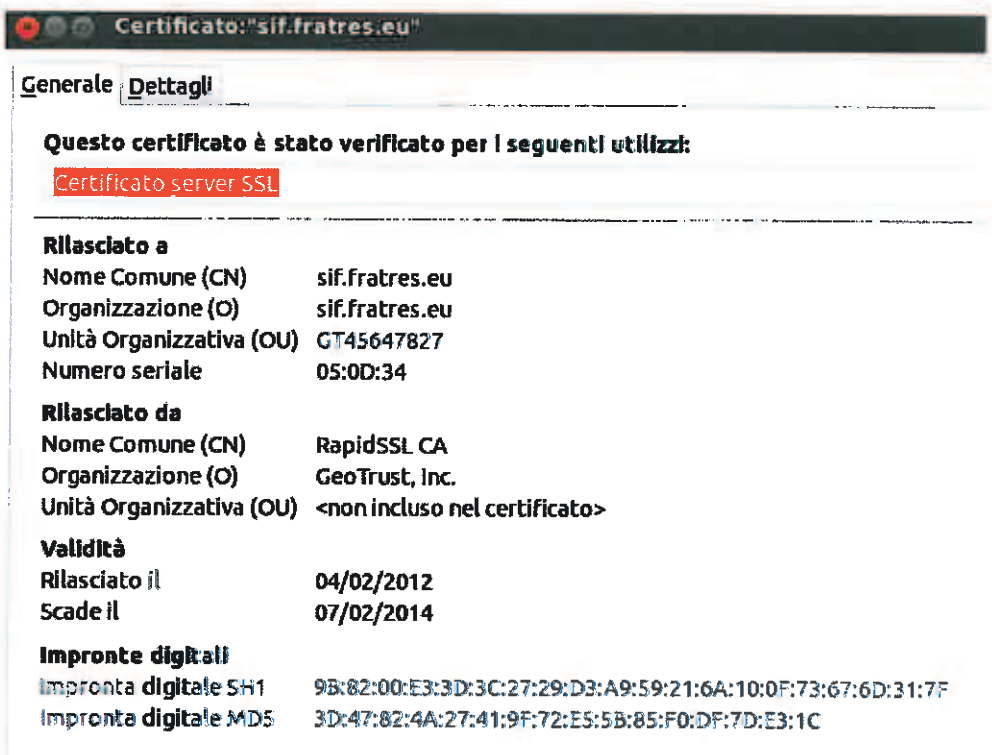
c) AGGIORNAMENTO PERIODICO DELL'INDIVIDUAZIONE DELL'AMBITO DEL TRATTAMENTO CONSENTITO AI SINGOLI INCARICATI E ADDETTI ALLA GESTIONE O ALLA MANUTENZIONE DEGLI STRUMENTI INFORMATICI

Ai sensi del punto 15 dell'Allegato B l'aggiornamento periodico descritto dalla lettera d) dell'art. 34 del Codice deve avvenire con cadenza almeno annuale. Occorre cioè che il Responsabile del trattamento verifichi, almeno una volta all'anno, l'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

d) PROCEDURE PER LA CUSTODIA DI COPIE DI SICUREZZA, IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI E DEI SISTEMI

Poiché la perdita dei dati dovuti a blocco del sistema informatico, è meno infrequente di quanto si possa pensare, è prevista l'effettuazione di copie di *back-up* degli archivi contenenti i dati. Questa operazione è effettuata direttamente dalla licenzataria della procedura, Genetrix srl, in base alla sottoscrizione di apposito contratto di assistenza e manutenzione.

Inoltre i profili assegnati al **livello nazionale, regionale e provinciale** sono tali da non poter gestire in nessun modo i dati dei soci dei singoli Gruppi; possono unicamente consultare la reportistica per numeri. Il caso particolare può essere che un Presidente di Organo consociativo sia anche Presidente di Gruppo: in questo caso le credenziali di autenticazione saranno identiche e la persona ha la facoltà di scegliere il livello di gestione che comunque tiene traccia dell'autorizzazione prescelta.


Certificato:"sif.fratres.eu"

Generale | Dettagli

Questo certificato è stato verificato per i seguenti utilizzi:

Certificato server SSL

Rilasciato a	
Nome Comune (CN)	sif.fratres.eu
Organizzazione (O)	sif.fratres.eu
Unità Organizzativa (OU)	GT45647827
Numero seriale	05:0D:34
Rilasciato da	
Nome Comune (CN)	RapidSSL CA
Organizzazione (O)	GeoTrust, Inc.
Unità Organizzativa (OU)	<non incluso nel certificato>
Validità	
Rilasciato il	04/02/2012
Scade il	07/02/2014
Impronte digitali	
Impronta digitale SH1	9B:82:00:E3:3D:3C:27:29:D3:A9:59:21:6A:10:0F:73:67:6D:31:7F
Impronta digitale MD5	3D:47:82:4A:27:41:9F:72:E5:5B:85:F0:DF:7D:E3:1C