# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
# (DPS)

*(Art. 34, comma 1, lettera g del D.Lgs. n°196/2003 e regola 19 dell'allegato "B" del medesimo decreto)*

31/03/2017

Avis Comunale Milazzo

# - DPS –

## *DOCUMENTO PROGRAMMATICO SULLA SICUREZZA*

*(Redatto ai sensi dell'art. 34, comma 1, lettera g del D. Lgs. n° 196/2003*
*e regola 19 dell'allegato "B" del medesimo decreto)*

L'AVIS Associazione Volontari Italiani sangue - sezione Comunale di Milazzo (ME) - C.F. 92003330831 con sede in 98057 Milazzo - Via On. Gaetano Martino 1 - premesso che nell'ambito della propria attività effettua trattamento di dati personali, come di seguito elencati, con il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, fisiche e logiche, previste per la tutela dei dati trattati.
In conformità con quanto prescritto al punto 19 del disciplinare tecnico (all. B, D.Lgs.vo n° 196/03) nel presente documento si forniscono idonee informazioni riguardanti:

**1)** Elenco e modalità dei trattamenti di dati personali (**regola 19.1 all. B**) mediante:
- individuazione tipologia dei dati personali trattati;
- descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
- elaborazione della mappa dei trattamenti effettuati.

**2)** Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (**regola 19.2 all. B**);

**3)** Analisi dei rischi a cui sono soggetti i dati (**regola 19.3 all. B**);

**4)** Misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati (**regola 19.4 all. B**);

**5)** Criteri di modalità di ripristino dei dati a seguito di distruzione o danneggiamento (**regola 19.5 all. B**);

**6)** Pianificazione degli interventi formativi previsti (**regola 19.6 all. B**);

**7)** Adozione misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno (**regola 19.7 all. B**);

**8)** Individuazione dei criteri da adottare per la cifratura, o per la separazione dai dati personali, dei dati idonei a rivelare lo stato di salute e la vita sessuale (**regola 19.8 all. B**).

## *1 - ELENCO E MODALITA' DEI TRATTAMENTI DI DATI PERSONALI*

***- Regola 19.1 all. B -***

### 1.1 Individuazione tipologie dei dati personali trattati.

A seguito dell'analisi compiuta sono stati individuati i seguenti trattamenti:

- dati sia comuni che sensibili relativi ai soci e ai candidati in atto per diventarlo;
- dati comuni relativi a fornitori;

### 1.2 Descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti.

#### 1.2.1 Aree e locali

- Il trattamento dei dati avviene nella sede di via On. Gaetano Martino 1 nel comune di Milazzo (ME), in zona periferica.
- I locali interessati sono dislocati al primo piano e l'accesso è controllato oltre che da sistema di chiusura a chiave anche da un portone di ingresso condominiale a cui si accede tramite cancelletto che delimita la proprietà. L'abbattimento delle barriere architettoniche permettono l'accesso allo stabile, come pure un elevatore per persone diversamente abili, oltre alle scale, asserve il piano ove è dislocata la struttura. Elenco delle persone autorizzate all'ingresso in sede, attraverso dotazione di chiavi, è riportato in apposito registro posto nell'archivio amministrazione nell'aria di segreteria. Addetti alle operazioni di pulizia o di manutenzione accedono e operano sotto sorveglianza ed indicazione di responsabili Avis. La pulizia nei locali avviene solo con armadi chiusi e computer spenti o in stand-bay, protetti da password e sempre alla presenza di un incaricato al trattamento dei dati.
- Le finestre sono provviste di serrande senza passanti di sicurezza antisollevamento. Inoltre sui lati nord e sud sono presenti due uscite di sicurezza che attraverso scale esterne immettono nelle strade prospicienti di via On. G. Martino e via Maio Mariano.
- E' presente un sistema di allarme anti intrusione con sirena esterna ed un sistema di video sorveglianza.

#### 1.2.2 Schedari ed altri supporti cartacei

I supporti cartacei sono raccolti in schedari, all'interno di armadi, con chiusura a chiave a loro volta custodite in una cassetta di sicurezza vincolata sulla parete del locale adibito a visite mediche. Pertanto l'area è sempre sotto controllo medico nelle attività di routine e dei volontari autorizzati alla gestione documentale. Tali supporti contengono dati sensibili di donatori attualmente in attività e dati sensibili di donatori non più attivi per le motivazioni indicate nella cartella e conservati ai sensi dell'art. 16, commi c-d. A tali schedari accedono medici e solo personale volontario espressamente autorizzato, mediante chiave allocata in una cassetta centrale di sicurezza, vincolata alla parete, e posta nel locale segreteria. Altri supporti cartacei relativi ai fornitori di beni e servizi (Fatturazioni e dati comuni) per le attività amministrative sono custoditi, nell'aria di segreteria, nell'apposito armadio e vi accedono le persone autorizzate e preposte all'attività. Chiavi di accesso agli armadi infermieristici sono poste in una cassetta di sicurezza vincolata al muro della sala e la cui chiave è sempre posizionata nella cassetta di sicurezza centrale in segreteria. Elenco di personale in possesso di chiavi d'accesso è posto nella sala Presidenza.

### 1.2.3 Elaboratori non in rete

E' presente un elaboratore non in rete, fornito dal SIMT, solo nelle attività di raccolta.

### 1.2.4 Elaboratori in rete privata

E' presente un elaboratore in rete privata per l'interfacciamento del software di gestione sanitaria del donatore con gli strumenti di prelievo. Tali strumenti sono costituiti dalle bilance di prelievo e da un PC è fornito dal SIMT contenente dati sanitari dei donatori della sezione Tale attività, temporale, è attuata nelle giornate e ore previste per la raccolta sangue (attività istituzionale). La rete interna, attraverso access-point, provvede al trasferimento dei dati sanitari, rilevati dalla bilance durante il prelievo, al programma di gestione EmoNet installato virtualmente sul PC portatile dal Centro Trasfusionale. L'uso programmato della rete privata interna cesserà nel momento in cui sarà attivato il collegamento in rete internet con il Centro Trasfusionale eliminando il trasferimento dati sul PC portatile dello stesso Centro Trasfusionale. Sono presenti, inoltre, n°4 PC e tutti dispongono di collegamento ad Internet. Sono collegati in rete wireless e il Server per il salvataggio dei dati oggetto di trattamento è collocato sulla rete internet. La rete wireless è protetta da password e non è accessibile dall'esterno. Il portatile viene utilizzato anche per scopi didattici nelle conferenze esterne e non vi sono inseriti dati sensibili installati.

### 1.2.5 Elaboratori in rete pubblica

Non vi sono elaboratori in rete pubblica

### 1.2.6 Impianti di video sorveglianza

E' presente un sistema di video sorveglianza attivo 24 ore su 24 con registrazione degli eventi per 28 giorni consecutivi a ripetizione ciclica. Il sistema dotato di chiavi elettroniche codificate per nome della persona assegnataria, registra le attivazioni/disattivazioni del sistema della chiave utilizzata. E' possibile la sorveglianza a distanza attraverso una APP sul telefonino di sede o su quello del Legale Rappresentante (inserzione/disinserzione e controllo riprese telecamere) .

## 1.3 <u>Elaborazione della mappa dei trattamenti effettuati</u>

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

| Tipologia trattamento | Cartaceo | PC non in rete | PC in rete privata | PC in rete pubblica | Video-sorveglianza |
|---|---|---|---|---|---|
| Dati comuni relativi a soci donatori | X | | X | | |
| Dati comuni relativi a fornitori | X | | X | | |
| Dati comuni relativi ad altri soggetti | | | | | |
| Dati biometrici relativi a soci donatori | | | | | |
| Dati idonei a rilevare la posizione di persone/ oggetti | | | | | |
| Dati relativi allo svolgimento di attività economico/commerciali | | | | | |
| Dati di natura giudiziaria | | | | | |
| Dati di natura sensibile relativi a soci donatori o donatori sospesi | X | | | | |
| Dati idonei a rivelare lo stato di salute e la vita sessuale | X | | X (temporaneo) | | |

### 1.3.1 Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati, emerge che:

- Dati comuni relativi ai Donatori vengono trattati sistematicamente su supporti cartacei e con strumenti di elaborazione;
- I dati sensibili dei Donatori vengono trattati prevalentemente su supporti cartacei. Le analisi relative ai controlli periodici che alla donazione, contenenti dati sensibili, sono prelevate, dal centro trasfusionale, da persone incaricate e trasferite in busta chiusa nelle sede dell'Associazione. Dopo valutazione del Direttore Sanitario o del Responsabile UdR una copia è inserita nella cartella personale del donatore mentre l'originale è inoltrata al donatore via e-mail in forma crittografata o via P.T. previa autorizzazione presente nella domanda di iscrizione e rilevabile dal data-base AssoAvis. Pertanto si ribadisce che nessun dato sensibile viene archiviato sul PC o su programmi di elaborazione, in quanto quello utilizzato non permette la separazione di tali dati non avendo la possibilità di credenziali di accesso diverse per dati anagrafici e dati sensibili né tantomeno di possibilità di crittografarli se non nella solo fase di trasmissione.
- Dati sensibili sono inseriti nel sistema di gestione sanitaria del SIMT (denominato EmoNet) e nel momento in cui il sistema sarà posto sulla rete telematica solo medici autorizzati e forniti di credenziali potranno accedervi.
- La gestione dei dati del donatore operata tramite il programma "AssoAvis" permette, in ogni caso, la sola indicazione del gruppo sanguigno, comune ad una larga fascia di donatori, per cui elemento non identificabile del singolo donatore.
- Inoltre in sala prelievi, negli armadi sanitari è presente il registro farmaci su cui sono annotati eventuali utilizzi ai donatori soggetti a reazioni avverse durante e dopo la donazione. Gli armadi sono accessibili a medici, infermieri e personale autorizzato attraverso chiavi posti in una cassetta di sicurezza in segreteria.
- Dati comuni sui fornitori di beni e servizi (Fatturazioni e riferimenti amministrativi) solo su supporti cartacei.

## *2 - DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI.*

***- Regola 19.2 all. B -***

### 2.1 Titolare del trattamento dei dati

Per il trattamento dei dati personali, il legale rappresentante dell'Associazione, titolare del trattamento, Sig.or Silvestri Federico non ha nominato un Responsabile assumendo egli stesso il ruolo di gestire e mantenere in efficienza le misure di sicurezza previste dal s D.Lgs. 30/06/2003 n°196. Il sottoscritto per precedenti attività svolte, fornisce le garanzie previste dall'art. 29, comma 2 del D.Lgs. 30/06/2003 n°196. Lo stesso ha progettato, realizzato e mantenuto in efficienza le misure di sicurezza previste dal sopracitato decreto in quanto prima di ricoprire il ruolo di legale rappresentante è stato il Responsabile del trattamento nel precedente mandato. Si rammenta che il Titolare/Responsabile del trattamento non può delegare o demandare compiti di vigilanza sul rispetto da parte degli incaricati, da Lui nominati, delle istruzioni impartite.

## 2.2 Soggetti incaricati

Il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formale incarico da parte del Titolare/Responsabile mediante designazione per iscritto con il quale si individua l'ambito del trattamento consentito. Il livello di accessibilità nel software di gestione è impostato nel software stesso di concerto tra il Titolare/Responsabile del trattamento e l'Amministratore del sistema di sicurezza informatica.

## 2.3 Istruzioni specifiche fornite ai soggetti incaricati

Oltre alle istruzioni generali su come devono essere trattati i dati personali, agli incaricati sono fornite specifiche istruzioni relativamente a:

- Procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili osservando le maggiori cautele di trattamento che questi dati richiedono;
- Modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia e l'archiviazione degli stessi;
- Modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici e ai software e ai dati in essi contenuti. Elenco delle persone autorizzate attraverso password d'accesso ai sistemi elettronici è riportato in apposito registro nell'archivio amministrazione nell'aria di segreteria;
- Prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro;
- Procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- Procedure per il salvataggio dei dati;
- Modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali;
- Aggiornamento continuo utilizzando i materiali e gli strumenti relativi alle misure di sicurezza messi a disposizione dall'Associazione.

# *3 – ANALISI DEI RISCHI CHE INCOMBONO SUI DATI*

***- Regola 19.3 all. B -***

L'analisi dei possibili rischi che gravano sui dati è stata effettuata combinando due tipi di rilevazioni:

- la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- le caratteristiche degli strumenti utilizzati per il trattamento dei dati.

## 3.1 Strumenti impiegati nel trattamento

Sono stati individuati come sorgenti soggetti a rischio le seguenti categorie di strumenti utilizzati per il trattamento:

***Legenda***

- Schedari e altri supporti cartacei custoditi nell'area controllata; **A**
- Elaboratori in rete privata. **B**

| Fattori di rischio | Basso | Medio | Elevato |
|---|---|---|---|
| Rischio d'area legata all'accesso non autorizzato nei locali | A - B | | |
| Rischio guasti tecnici hardware e software | B | | |
| Rischio penetrazione nelle reti di comunicazioni | | B | |
| Rischio legato ad errori umani | A - B | | |
| Rischio d'area per possibili eventi distruttivi (Incendio – Furto – distruzione supporti di memoria - | **A** | **B** | |

## *4 - MISURE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI*

***- Regola 19.4 all. B -***

Alla luce dei fattori di rischio e delle aree individuate, nel presente paragrafo vengono descritte le misure atte a garantire:

- La protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- La corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- La sicurezza logica, nell'ambito degli strumenti elettronici.

Le successive misure indicate a sostegno della fase di protezione dei dati si suddividono in:

- Misure già adottate al momento della stesura del presente documento;
- Ulteriori misure finalizzate ad aumentare il livello di sicurezza del trattamento dei dati.

### 4.1 Protezione di aree e locali

Per quanto concerne il rischio che i dati vengano danneggiati o perduti a seguito di eventi distruttivi, i locali ove si svolge il trattamento dei dati sono protetti da:

- gruppi di continuità della corrente elettrica per gli elaboratori;
- estintore ad intervento manuale per i locali

## 4.2 Custodia e archiviazione dei dati

Agli incaricati sono state impartite istruzioni per la gestione, la custodia e l'archiviazione dei documenti e dei supporti. In particolare sono state fornite direttive per:

- Il corretto accesso ai dati personali sensibili;
- La conservazione e la custodia di documenti, atti e supporti contenenti dati personali sensibili. In particolar modo all'elenco dei donatori riportante il gruppo sanguigno ai fini delle chiamate alla donazione presso il Centro Trasfusionale dell'Ospedale di Milazzo, elenco che sarà successivamente distrutto dopo l'elaborazione di quello più aggiornato, che dovrà essere conservato nel locale archivio;
- La definizione delle persone autorizzare ad accedere ai locali archivio e le modalità di accesso.

## 4.3 Misure logiche di sicurezza

Per il trattamento effettuato con strumenti elettronici si sono individuate le seguenti misure:

- Realizzazione e gestione di un sistema di autenticazione informatica al fine di accertare l'identità delle persone che hanno accesso agli strumenti elettronici;
- Autorizzazione e definizione delle tipologie di dati ai quali gli incaricati possono accedere e utilizzare ai fine delle proprie mansioni lavorative;
- protezione di strumenti e dati da malfunzionamenti e attacchi informatici;
- Prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili, contenenti dati personali.
- Protezione dei dati gestionali dell'Associazione su server internet e hard-disk esterno di back-up.

### 4.3.1. Accesso ai dati e istruzioni impartite agli incaricati

Gli incaricati al trattamento dei dati dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- Obbligo di custodire i dispositivi di accesso agli strumenti informatici ( Username e Password per gli elaboratori e software) e modifica trimestrale;
- Obbligo, per l'Amministratore del sistema informativo, di trascrivere username e password in busta chiusa da depositate nell'armadio di backup. Titolare e/o Responsabile del trattamento avranno accesso al documento in caso di necessita;
- Obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento e gli armadi contenenti le schede sanitarie;
- Obbligo di non lasciare incustodita la cartella clinica su cui si sta operando ed elenco gruppi sanguigni utilizzato per le chiamate;
- Obbligo di distruzione di copie, documenti ed elenchi obsoleti e senza obbligo di conservazione nel tempo;
- Obbligo di verificare la chiusura degli armadi contenenti le schede sanitarie e la relativa cassetta di sicurezza di deposito delle stesse chiavi;
- Obbligo di assoluta riservatezza;
- Divieto di divulgazione delle password di accesso ai sistemi.

### 4.3.2 Protezione di strumenti e dati

Premesso che non vengono trattati dati sensibili in rete, il sistema di elaborazione è comunque protetto da programmi antivirus e di sistemi firewall anti-intrusione.
Il sistema è altresì impostato per l'aggiornamento periodico automatico delle protezione.
Agli incaricati è stato affidato, in ogni caso, il compito di verificare e aggiornare con periodicità mensile sia i sistemi operativi e di protezione, con le opportune patch di sicurezza, sia i programmi antivirus e firewall.
Inoltre una cartella di archivio su cui sono salvati tutti i file di lavoro dell'Associazione è presente su rete internet, protetta da password, garantendo la sua sicurezza e il suo recupero in caso di anomalie del PC o di distruzione accidentale o dolosa.

### 4.3.3 Supporti rimovibili

La tutela dei dati personali su supporti rimovibili è articolata come segue:

- Custodia dei supporti (Hard-disk esterno rimovibile di backup dati, DVD di ripristino) in armadio chiuso a chiave in locale controllato e accessibile solo a persone autorizzate;
- Cancellazione dei dati obsoleti (donatori cessati, trasferiti etc.) dal supporto rimovibile una volta cessate le ragioni per la conservazione. La copia dei dati sensibili riferiti alle analisi sulla donazione del donatore, inserita nulla sua cartella personale, viene conservata secondo i termini di legge, mentre nel caso delle cessazioni sopra indicate l'intera cartella è archiviata in una sezione dedicata. Da tener presente che tutti i dati sanitari riferiti ai donatori ed alle donazione trovano archiviazione nel data-base (EmoNet) del centro trasfusionale dell'ospedale di Milazzo.

## 5 – *CRITERI E MODALITA' DI RIPRISTINO DATI*
***- Regola 19.5 all. B -***

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati personali presenti. Il salvataggio di tali dati avviene con frequenza settimanale e le relative copie, su Hard-disk esterno rimovibile, vengono custodite in un armadietto chiuso a chiave posto nella sala segreteria. Tuttavia tutti i dati sono conservati sin dall'inizio su supporti cartacei, anch'essi opportunamente conservati nel locale archivio dati.
Le due procedure di archiviazione, complementari tra loro, sono adottate per il totale recupero dei dati in caso di perdita accidentale come indicato al punto 3.1. Da far presente che per la lettura dei dati necessita l'installazione dell'apposito programma AssoAvis o l'intervento di tecnici informatici.
Nessun problema si manifesta nel recupero dei dati gestionale dell'Associazione in quanto archiviati sul web, protetti da password, sono sempre disponibili. Anche per questi dati sono previste procedure di back-up, per l'utilizzo di lavoro in caso di indisponibilità della rete internet. I sistemi di salvataggio sono così riassunti:

| | |
|---|---|
| 1 | Internet |
| 2 | Copia cartacea |
| 3 | Back-up su hard-disk esterno |

## 6 – INTERVENTI FORMATIVI PREVISTI

**- Regola 19.6 all. B -**

Agli incaricati al trattamento, l'Associazione (direttamente o tramite soggetti delegati) fornisce la necessaria formazione:

- al momento della nomina a incaricato;
- in occasione dell'introduzione di nuovi strumenti e programmi informatici.

La formazione interesserà sia le norme generali in materia di privacy, sia gli aspetti peculiari dei trattamenti effettuati.

## 7 – AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

**- Regola 19.7 all. B -**

Nello svolgimento dell'attività non vengono affidati dati personali all'esterno. Solo dall'esterno, ovvero dal Centro Trasfusionale (SIMT di competenza), afferiscono le analisi riferite alla donazione veicolate da persone incaricate ai sensi della prevista normativa sia per il controllo del Direttore sanitario Avis sia e del Responsabile UdR e sia per l'invio ai donatori. Le analisi eseguiti contestualmente alla donazione (dati sensibili) e pervenute in sede, sono inoltrate via posta o e-mail crittografata previo consenso espresso dal donatore al momento dell'iscrizione. Da persone incaricate e dopo controllo medico. Eventuali patologie rilevate dalle analisi sono di competenza del SIMT il quale informa solo per la sospensione(temporanea) o esclusione (definitiva), informazione necessaria per l'aggiornamento del data-base. La natura della causa sospensiva (temporanea e definitiva) è riferita, in busta chiusa, solo al Responsabile UdR, il quale informa il medico addetto alla selezione dei donatori e il Direttore Sanitario Avis.

## 8 – INDIVIDUAZIONE DEI CRITERI DA ADOTTARE PER LA CIFRATURA

**- Regola 19.5 all. B -**

I dati comuni sono trattati su supporto elettronico e cartaceo.
Alcuni dati di idoneità alla donazione sono riportati su sistema elettronico utilizzando un programma specifico (AssoAvis) che non permette la separazione delle due fattispecie di dati come indicato al punto 1.3.1. Sono inoltre inseriti dati riferiti alla sospensione temporanea (inidoneità temporanea) stabilita dal Medico addetto alla selezionatore.

- Dati sensibili più specifici riguardanti la condizione fisica di idoneità alla donazione e analisi sulla donazione sono archiviati solo su supporto cartaceo e costituiscono la scheda sanitaria del donatore.
- Le schede sanitarie, su base cartacea, sono classificate e archiviate in armadi a comparti numerati le cui chiavi d'accesso sono custodite in una cassetta di sicurezza accessibile al medico e alle persone incaricate all'archiviazione.
- Sono trasmessi dati sensibili inerenti la donazione per via telematica mediante cifratura o via P.T., sempre su espressa autorizzazione.
- Dati comuni relativi ai fornitori di beni e servizi riportati su atti, documenti fatturazioni e bilanci etc. sono archiviati solo su base cartacea e conservati nell'armadio archivio amministrazione in sala

Presidenza. La cifratura è adottata solo per la trasmissione di dati sensibili riferiti ad analisi post-donazione. Nessun'altra cifratura è adottata per determinati trattamenti di dati idonei a rivelare lo stato di salute o aspetti della vita personale (sessuale, religiosa, politica etc.) in quanto l'AVIS non è un organismo sanitario ma un'Associazione di donatori volontari normata da uno statuto Nazionale e da quanto previsto dalla **legge n°107/90** e successivi decreti, ovvero disciplina sulle attività trasfusionali del sangue e suoi derivati, e dalla **legge quadro 266/91** sul volontariato.

## *NOTE E INDICAZIONI SULLE MODIFICHE APPORTATE*

### Tabella delle modifiche

**AGGIORNAMENTI DPS**

| Posizione | Data | Note sulle modifiche |
|---|---|---|
| Punto 1.2.5 | 31/03/2006 | |
| Planimetria | 31/03/2006 | |
| Punto 1.2.5 | 31/03/2008 | |
| Punto 1.3 | 31/03/2008 | |
| Punto 3.1 | 31/03/2008 | |
| Planimetria | 31/03/2008 | |
| Punto 1.3 | 31/03/2010 | |
| Punto 1.3.1 | 31/03/2010 | |
| Punto 4.3.3 | 31/03/2010 | |
| Punto 8 | 31/03/2010 | |
| Punto 0 | 01/08/2011 | Assetto interno |
| Punto 1.2.1 | 01/08/2011 | Assetto interno |
| Punto 7 | 01/08/2011 | Assetto interno |
| Planimetria | 01/08/2011 | Variazione sede sociale e legale |
| Punto 1.3.1 | 31/03/2013 | Assetto interno |
| Punto 2.1 | 31/03/2013 | Assetto interno |
| Punto 4.2 | 31/03/2013 | Assetto interno |
| Punto 4.3.3 | 31/03/2013 | Assetto interno |
| Punto 8 | 31/03/2013 | Assetto interno |
| Planimetria | 31/03/2013 | Adattamento locali per accreditamento Regionale |
| Planimetria | 31/03/2014 | Variazione n° civico |
| Punto 1.2.1 | 01/07/2014 | Assetto interno |
| Punto 1.2.2 | 01/07/2014 | Assetto interno |
| Punto 1.3.1 | 01/07/2014 | Assetto interno |
| Punto 4.3 | 01/07/2014 | Assetto interno |
| Punto 5 | 01/07/2014 | Assetto interno |
| Planimetria | 01/07/2014 | Variazione sede sociale e legale |
| Punto 1.2 | 31/03/2015 | Assetto interno |

Tabella delle modifiche

| AGGIORNAMENTI DPS | | |
|---|---|---|
| **Posizione** | **Data** | **Note sulle modifiche** |
| Punto 1.2.1 | 31/03/2016 | Assetto interno |
| Punto 1.2.3 | 31/03/2016 | Assetto interno |
| Punto 1.2.4 | 31/03/2016 | Assetto interno |
| Punto 1.2.5 | 31/03/2016 | Assetto interno |
| Punto 1.2.6 | 31/03/2016 | Assetto interno |
| Punto 1.2.4 | 31/03/2017 | Elaboratori in rete privata |
| Punto 5 | 31/03/2017 | Modalità di ripristino dati - tabella |

## *ELENCO ALLEGATI COSTITUENTI PARTE INTEGRANTE DEL DPS*

- Planimetria locali con disposizione archivi e strumentazioni utilizzata per i trattamenti
- Planimetria locali con disposizione sensori allarmi, telecamere, centralina e registrazioni.
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per la sicurezza informatica
- Lettera di incarico per l'amministratore di sistema

***Il presente Documento Programmatico sulla Sicurezza (DPS) deve essere divulgato e illustrato a tutti gli incaricati.***

---

**Il presente documento, il cui originale è custodito presso la sede dell'Associazione per essere esibito in caso di controllo, è soggetto ad aggiornamento obbligatorio entro il 31 marzo di ogni anno, ai sensi dell'art.19 allegato "B" del D.Lgs. 30/06/2003 n°196. Il documento deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:**

- **Modifiche all'assetto organizzativo ed in particolare del sistema informativo(sostituzioni hardware, software, procedure, connessioni di rete etc.) tali da giustificare una revisione del piano;**
- **Danneggiamento o attacchi al patrimonio informativo dell'associazione tali da rendere necessario correggere o aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio**.

**Ai sensi del punto 26 - Misure di tutela e garanzia - dell'allegato "B" del D.Lgs. 30/06/2003 n°196 il Titolare del trattamento ha l'obbligo di riferire, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.**

Milazzo lì 31/Marzo/2017

Il redattore del documento
(Federico Silvestri)

……
*(Firma)*

***Nota: fonti di documentazione***

- *D.Lgs. n°196 del 30/06/2003;*
- *Allegato "B" D.Lgs. n°196 - disciplinare tecnico di misure minime di sicurezza;*
- *Garante per la protezione dei dati personali;*
- *http//www.garanteprivacy.it;*
- *Internet – programmi in linea per stesura DPS. e sicurezza in rete.*