NOTE SULLA LA PROTEZIONE DEI DATI PERSONALI

Il **Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali** – Vigente dal 31 luglio 2004 - Convertito con la legge 27 luglio 2004, n. 188 ha come finalità la garanzia che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Alcune definizioni utili per comprendere meglio l'applicabilità di questo Decreto:

a**) "trattamento",** qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **"dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;

d**) "dati sensibili"**, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) **"dati giudiziari"**, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) **"titolare"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g)**"responsabile"**, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) **"interessato"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

GLI ADEMPIMENTI DI AVIS

Indipendentemente dal tipo di trattamento e di raccolta dei dati che viene effettuato dalla sede AVIS, serve precisare che:

- In AVIS il **Titolare** dei dati è il rappresentante legale, che è il Presidente dell'AVIS Si sottolinea che con il nuovo statuto, ogni associazione deve adottare il registro dei soci, pertanto, tutti i Presidenti, ad ogni livello, sono titolari di dati personali di terzi raccolti nell'ambito dell'attività dell'Associazione.
- Il Titolare può delegare un **Responsabile** al trattamento dei dati dei donatori, che sua volta, può autorizzare un **Incaricato** a compiere le operazioni di trattamento di dati.

- Questo sistema di delega: **Titolare, Responsabile, Incaricato**, in AVIS, si configura sicuramente là dove sono previsti degli impiegati, in questo caso, sarebbe utile che il Presidente delegasse, l'impiegato o il responsabile della struttura amministrativa, quale Responsabile del trattamento dei dati.
- Nel caso di Associazione senza personale dipendente, il Presidente può delegare quale responsabile il Consigliere che con maggiore frequenza opera sull'archivio dei donatori, oppure tenere per sé tutte le funzioni.
- Trattamento di dati per le AVIS Comunali, s'intende: la raccolta, l'aggiornamento, la conservazione e la consultazione dei dati personali e dei dati sensibili dei soci sia donatori, che non donatori e di eventuali impiegati; per le AVIS Provinciali, Regionali e per il Nazionale, ai dati di cui sopra, si aggiungono i dati riguardanti le persone giuridiche associate.
- Nel trattamento dei dati sono comprese anche le operazioni di chiamata del donatore, l'invio di comunicazioni, l'invio dei referti degli esami, l'elaborazione degli stipendi, nel caso in cui l'AVIS abbia dipendenti e gli stessi vengano elaborati all'interno dell'AVIS stessa, la stampa degli indirizzi per l'invio dei vari notiziari, in questo ultimo caso ci si deve garantire che il tipografo utilizzi gli indirizzi solo per l'invio dei Notiziari ai donatori e non per altri scopi, bisognerebbe essere inoltre certi che una volta utilizzati, gli indirizzi vengano cancellati dalle memorie informatiche della tipografia.

MISURE DI SICUREZZA

Il Titolare, o chi per esso, deve garantire misure minime di sicurezza, assicurando che i dati personali oggetto di trattamento vengano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nel caso in cui l'AVIS non sia dotata di strumenti elettronici per il trattamento dei dati, non la esime dal mettere in atto idonee misure di protezione.

Pertanto, in questo caso, i dati andranno custoditi in contenitori predisposti con sistemi di sicurezza e l'accesso sarà consentito solo alle persone autorizzate.

Per le AVIS dotate di strumenti informatici, si dovranno prevedere i seguenti sistemi di sicurezza:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Inoltre, nel caso in cui l'AVIS sia dotata di strumenti elettronici bisogna distinguere tra quelle AVIS che utilizzano il PC in monoutenza, cioè non connesso ad una rete, e quelle AVIS dotate di reti informatiche, collegate alle quali vi sono più PC o terminali non intelligenti.

MONOUTENZA

In questo caso è necessario che l'accesso al programma di gestione dei donatori sia consentito utilizzando una Username (Codice utente) e una Password, che deve essere di otto caratteri e deve avere una scadenza almeno semestrale.

Solo il responsabile deve conoscere Username e Password e solo a lui è consentito modificare la password.

Username e Password sono le credenziali di autenticazione.

SISTEMI IN RETE

Le AVIS che effettuano la raccolta oppure AVIS di coordinamento per la gestione dei donatori, possono avere la necessità di essere dotate di un sistema che consenta a più utenti di connettersi contemporaneamente ad un Server non solo per l'accesso all'archivio dei donatori, ma anche ad altri programmi. In questo caso, quasi sicuramente vi saranno più impiegati nell'AVIS, per cui oltre al Responsabile, vi saranno anche degli Incaricati.

Il programma deve prevedere, per ognuno, l'utilizzo di Username e Password per l'accesso al programma, inoltre, l'amministratore del sistema deve prevedere il divieto di accesso al Server senza autorizzazione, generalmente detto accesso è consentito solo al System Administrator.

Più complesso è il caso in cui l'AVIS utilizzi la rete Aziendale dell'AUSL per la gestione dei propri archivi; la responsabilità di accesso al Server dell'AUSL, da parte di estranei, deve essere garantita dal responsabile del trattamento dei dati dell'Azienda Ospedaliera, mentre quella di accesso al programma deve essere garantito dal responsabile.

In questo caso si configura una doppia responsabilità, sarebbe quindi opportuno che la Convenzione "Azienda Ospedaliera - AVIS" preveda la regolamentazione di accesso al Server con i vari criteri di autorizzazione e che siano indicati i responsabili dei trattamenti dei dati sia per l'Avis che per l'Azienda Ospedaliera.

In tutti i casi, è evidente, che nel momento in cui si abbandona la postazione di lavoro, è necessario chiudere il programma di gestione dei donatori, come pure si raccomanda di non attaccare al video del PC Post-it con i codici di autorizzazione, altrimenti tutte le tecniche di riservatezza risulterebbero inutili; chiudere e riaprire un programma comporta tempi molto limitati che non aggravano sicuramente il lavoro. Si sottolinea che la cura nel mantenere la segretezza della Username e della Password, deve essere pari a quella con la quale si custodisce il codice bancomat.

TIPOLOGIA DI DATI E LORO GESTIONE

Come si è detto più sopra i dati gestiti dalle AVIS sono di due tipi:

1. Personali
2. Sensibili

Per dati personali si intendono oltre ai dati anagrafici, quelli che consentono la chiamata per il prelievo e i dati associativi;

Per dati sensibili si intendono di dati di carattere sanitario, cioè: Gruppo, Fattore Rh, Kell, motivi di sospensione, referti degli esami, eventuali allergie, e quanto altro attenga ad individuare la salute del donatore.

Per i primi dati non vi sono particolari problemi nel loro trattamento, se non quello della correttezza e della sicurezza, per i secondi, invece è necessario adottare "tecniche di cifratura o di codici identificativi per determinati trattamenti"; ad esempio: Gruppo, fattore Rh, potrebbero essere cifrati; i motivi di sospensione potrebbero essere identificati attraverso una codifica, la cui lettura in chiaro dovrebbe essere o all'esterno del Data Base oppure essere cifrata.

Questa tecnica detta anche crittografica, consente a chi è autorizzato di accedere al Data base, ed avere tutte le informazioni in chiaro, invece ad eventuali intrusi di avere a disposizione solo cifre senza alcun senso.

In alternativa al metodo della cifratura, il decreto prevede la possibilità, come misura minima di sicurezza lo sdoppiamento dell'archivio in due o più Data base, legati tra loro da una codifica che consente la lettura abbinata dei dati.

Questo problema ha dato vita a diversi Convegni, Seminari, ecc. tra i vari responsabili di gestione di dati sensibili, in particolare nell'ambiente sanitario, in quanto la crittografia, oltre ad aver un costo di tutto rispetto, ha bisogno anche di elaboratori più performanti di quelli in uso, in particolare presso le sedi AVIS, con costo più elevato.

Ma la cosa che preoccupa è la necessità di dover convertire tutte le procedure sia per quanto riguarda l'hardware, sia per quanto riguarda il software, per cui al momento si stanno cercando di adottare le misure minime di sicurezza.

Se tutto questo rappresenta un serio problema per organizzazioni complesse e strutturate, possiamo immaginare cosa possa rappresentare per una Associazione quale l'AVIS, dislocata su tutto il territorio Nazionale, con strutture anche molto piccole e, spesso, senza l'ausilio di personale dipendente.

Di seguito si indicano alcuni consigli utili per adeguarsi alla normativa.

ASSOAVIS

Il programma di gestione dei donatori messo a disposizione dall'AVIS Nazionale ha già un buon livello di protezione, in quanto i dati sensibili sono già in formato tabellare, per cui eventuali intrusi hanno bisogno di conoscere la dislocazione delle tabelle per poterle leggere e poi, l'intruso, potrà decodificare i dati e quindi conoscere per ogni donatore il valore dei dati sensibili.

E' una operazione complessa che solo chi ha una buona conoscenza del computer ed in particolare dei programmi usati per la gestione del Data Base, può compiere, ciò nonostante non basta a soddisfare le richieste della normativa, per questi motivi, la Mesis, che ha prodotto il programma, su richiesta dell'AVIS Nazionale, sta predisponendo un progetto per la crittografia dei soli dati sensibili.

In questo modo non sarà più possibile, per un intruso anche molto esperto, conoscere il valore dei dati di cui sopra.

I dati in oggetto sono pochi, quindi non si dovrà procedere a conversioni dispendio sia dal punto di vista economico che da quello delle risorse umane, sarà sufficiente scaricare dal sito della Mesis l'aggiornamento di Assoavis ed eseguire il programma.

Come si è detto in precedenza l'intrusione può essere possibile anche attraverso la rete dell'Azienda Ospedaliera, qualora Assoavis sia allocato su una elaboratore dell'Azienda e l'AVIS utilizzi la rete della medesima.

Nel progetto che la Mesis sta predisponendo, sarà inoltre rafforzato il sistema autorizzativo di accesso al programma, adottando una password di 8 caratteri, con validità semestrale, la modifica della quale potrà essere effettuata solo dall'utilizzatore autorizzato del programma.

Le modifiche di cui sopra ad Assoavis saranno apportate solo alla versione 5, per cui tra le cose da fare da parte degli utenti che non la utilizzano, sarà necessario, migrare dalla versione in uso alla versione 5.

Il costo delle modifiche, come già per gli altri aggiornamenti, saranno a carico dell'AVIS Nazionale, proprietaria del programma; con ogni probabilità questo è il momento di allinearsi all'ultima versione.

Come è stato comunicato a suo tempo il passaggio alla nuova versione costa solo € 50 più spese di spedizione; mentre il costo si riduce a € 25 per gli utenti che hanno un contratto di assistenza sul vecchio "Assoavis".

Le modalità per richiedere la nuova versione, dovrebbero essere note, e comunque è sufficiente contattare la Sig.na Giardina Luisa della Sede Nazionale.

UTILIZZATORI DI ALTRI PROGRAMMI

Le AVIS che utilizzano programmi propri, dovranno prendere accordi con il programmatore o con la software house che ha realizzato il loro programma per apportare le modifiche necessarie al fine di garantire il rispetto delle norme previste dal Decreto; le modifiche sostanzialmente dovrebbe essere quelle elencate più sopra per Assoavis.

Le AVIS di cui sopra, potrebbero valutare l'opportunità di migrare ad Assoavis, sapendo che i costi sono quelli sopraindicati ai quali si dovrà aggiungere il costo del programma di conversione che potrà essere sviluppato dalla Mesis, e che gli aggiornamenti sono a carico dell'AVIS Nazionale.

Documento programmatico sulla sicurezza (DPS)

(Codice in materia di protezione dei dati personali
art. 34 e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196)

Il DPS è un documento che deve essere redatto dal titolare del trattamento dei dati, nel caso dell'AVIS dal legale rappresentante, e deve fare parte integrante della relazione accompagnatoria al Bilancio consuntivo.

Per l'anno 2004 e per l'AVIS che con ogni probabilità lo redigerà per la prima volta, poiché con la normativa precedente non era tenuta a compilarlo, la data di presentazione è il 30 giugno 2005, anziché il 31 marzo, dal prossimo anno, il DPS dovrà essere compilato entro il 31 marzo.

IL legislatore ha introdotto questa regola per rendere meglio edotti gli organi di vertice e responsabilizzarli in materia di sicurezza.

Il DPS è costituito da una serie di tabelle; di seguito si elencano le tabelle che dovrebbero interessare alle AVIS, in particolare a quelle che utilizzano Assoavis (quelle che utilizzano programmi diversi dovranno sostituire il nome di MSDE - Assoavis con quello usato (per molte AVIS le tabelle sotto riportate sono il DPS).

Il contenuto delle colonne delle tabelle, scritto in corsivo, andrà modificato secondo le esigenze, quello che si riporta e esemplificativo, ma comunque sufficientemente realistico, in base alle nostre conoscenze della Associazione.

Nel caso in cui l'AVIS gestisca anche altre informazioni diverse dai donatori si dovranno indicare anche la descrizione di tali dati, per esempio se l'AVIS è dotata di dipendenti si dovrà indicare che il trattamento dei dati riguarda i dipendenti per i quali si fanno le paghe; si dovrà quindi indicare se l'archivio informatico o cartaceo è presso la sede dell'AVIS oppure presso uno studio che fa stipendi.

Di seguito si allega una ipotesi di DPS, che per molte Avis che utilizzano Assoavis può essere duplicato, cambiando ovviamente la denominazione dell'Avis e dei responsabili.

ASSOCIAZIONE VOLONTARI ITALIANI SANGUE

AVIS

DPS – Documento Programmatico sulla Sicurezza

Ex D.Lgs. n. 196/2003 - All.B. regole 19.x

Premessa

Il presente documento corrisponde al dettato del D.Lgs. N. 196/2003 in particolare a quanto indicato al: "Titolo V – Sicurezza dei dati-, capo II – misure minime di sicurezza-.

Art. 31
(Obblighi di sicurezza)
I dati personali oggetto di trattamento sono custoditi e controllati, anche in elazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

Art. 33
(Misure minime)
Nel quadro dei più generali obblighi di sicurezza di cui allrt. 31, o previsti da speciali disposizioni, il titolare del trattamento è comunque tenuto ad adottare le misure minime individuate nel presente capo o ai sensi dell'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34
(Trattamento con strumenti elettronici)
Il trattamento dei dati personali effettuato con strumenti elettronici è consentito in quanto sono adottate le seguenti misure minime:

a) Autenticazione informatica;
b) Adozione di procedure di gestione delle credenziali di autenticazione;
c) Utilizzazione di un sistema di autorizzazione;
d) Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) Adozione di procedure per la custodia di copie di sicurezza; adozione di tecniche di cifratura per determinati trattamenti di dati idonei a rivelare lo stato di salute.

L'Avis ha pertanto corrisposto a quanto previsto dalla norma adottando il presente **"Documento Programmatico sulla Sicurezza"**
La stesura del documento si è basata su quanto suggerito dal garante nella "guida operativa per redigere il Documento Programmatico sulla sicurezza, pubblicata sukl sito ufficiale del garante in versione definitiva in data 11.6.2004; le tabelle, che costituiscono parte integrante e sostanziale del presente documento, sono state predisposte e compilate in corrispondenza della Guida Operativa.

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali

Descrizione sinteca del trattamento		Natura dei dati trattati	Struttura di riferimento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati			
Gestione donatori di sangue	*Donatori volontari di sangue*	*Sensibili*	*Associazione Volontari Italiani di Sangue*	*Personal Computer **
**nel caso in cui presso l'AVIS vi sia una rete di PC si dovrà descrivere per Esempio: 1 server con 2 Client; oppure se si utilizzano terminali non intelligenti collegati ad un elaboratore si dovrà scrivere Mainframe (tecnologia in disuso), oppure sistema UNIX*				

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti

Codice	Identificativo del trattamento	Eventuale Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione
1	*Chiamata dei donatori per la donazione*	*Assoavis*	*Sede AVIS **	*PC ***	*****
2	*Ricerca di donatori per varie tipologie*	*Assoavis*	*Sede AVIS **	*PC ***	*****
3	*Invio di comunicati vari*	*Assoavis*	*Sede AVIS **	*PC ***	*****
** Se viene utilizzato il PC di un Consigliere si dovrà indicare la sede dell'Abitazione del Consigliere presso il quale vengo fatte le elaborazioni*					
*** se per la gestione dei donatori si utilizza un elaboratore al quale sono connessi terminali non intelligenti si dovrà scrivere: terminali non intelligenti (tecnologia in disuso) ovviamente ciò dovrà essere coerente con la tabella precedente*					
**** se si usa un solo PC si scriverà nessuna, se utilizza una un server con 1 o più client si scriverà rete locale*					

Tabella 2 - Competenze e responsabilità delle strutture preposte ai trattamenti

Struttura	Codici dei trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
AVIS	*1,2,3.*	*Acquisizione e caricamento dei dati, consultazione, aggiornamento, comunicazione ai donatori, indagini statistiche per tipologia di datisaltaggi e ripristini **
** Nel caso in cui la gestione vera e propria sia effettuata per esempio dall'AVIS Provinciale e le AVIS Comunali o di Base acquisiscano solo i dati per la consulatazione e l'invio di comunicazione non si dovranno indicare le funzioni: caricamento dati e aggiornamento*		

Tabella 3- Analisi dei rischi

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamento degli operatori	Sottrazione di credenziali di autenticazione	*SI*	*bassa (in quanto i dati sensibili sono pochissi e di nessun rilievo ai fini della salute dei donatori*
	Carenza di consapevolezza, disattenzione o incuria	*SI*	*bassa (vedi sopra)*
	Comportamenti sleali o fraudolenti	*NO*	*In quanto lo statuto dell'AVIS vincola ad un suo corretto delle risorse e quindi dei soci*
	errore materiale	*SI*	*bassa (facilità di ripristino)*
	Altro evento		
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	*SI*	*Bassa (facilità di ripristino)*
	Spamming o tecniche di sabotaggio	*NO*	*In quanto i dati non sono di interesse da valorizzare un sabotaggio*
	Malfunzionamento, indisponibilità o degrado degli strumenti	*SI*	*Bassa (facilità di ripristino)*
	Accessi esterni non autorizzati	*NO*	*PC non in rete **
	Intercettazione di informazioni in rete	*NO*	*PC non in rete **
	Altro evento		
Eventi relativi al contesto	Accessi esterni non autorizzati ai locali	*SI*	*Bassa (facilità di ripristino)*
	Sottrazione di strumenti contenenti dati	*SI*	*Bassa (facilità di ripristino)*
	Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria	*SI*	*Bassa (facilità di ripristino)*

	Guasto ai sistemi complementari (impianto elettrico, climatizzatore, ecc)	*SI*	*Bassa (facilità di ripristino)*
	errori umani nella gestione della sicurezza fisica	*SI*	*Bassa (facilità di ripristino)*
	altro evento		
** Queste risposte posso soddisfare anche le AVIS che hanno reti locali, in quanto dall'esterno possono accedere solo se si utilizzano reti geografiche, cioè tra più insediamenti*			

Tabella 4.1 – Le misure di sicurezza adottate o da adottare

Misure	Descrizione dei rischi contrastati	Codici dei Trattamenti interessati	Misure già in essere	Misure da adottare	Struttura o persone addette all'adozione
Sistema di autenticazione informatica	*impedire l'accesso agli intrusi*	*1,2,3*		*SI*	*AVIS*
Sistema di cifratura	*rendere inaccessibili i dati sensibili*	*1,2,3*		*SI*	*AVIS*

Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati

Ripristino		
Banca/data base/archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
MSDE / Assoavis	*Giornalmente con procedura prevista dall'applicativo*	*Mensilmente*

Tabella 6 – Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	Classi di incarichi o tipologie di incaricati interessati	tempi previsti
Corsi sull'utilizzo di Assoavis	*Soci volontari dell'AVIS che utilizzano Assoavis*	*A richiesta, se necessario, in quanto il manuale è sufficientemente esplicativo anche per non addetti ai lavori*

Tabella 8 – Cifratura dei dati

Codici trattamento dati	Protezione scelta	Tecnica adottata	
		Descrizione	Informazioni utili
1,2,3	*cifratura*	*Microsoft Base Crytographic Provider v1.0*	*La crittografia dei valori contenuti nei campi è eseguita mediante le funzioni base di crittografia di Windows utilizzando le funzionalità contenute nelle librereie denominate comunemente "Cypto Api".*

Al termine di questa lunga circolare, per coloro che fossero interessati ad approfondire l'argomento possono visitare le pagine del sito: www.garanteprivacy.it : normativa/italiana/ il codice in materia di protezione dei dati personali; inoltre, la pagina Fac-simili e adempimenti/Documento programmatico sulla sicurezza/Guida operativa per redigere il documento programmatico sulla sicurezza – 11giugno 2004.pdf; i documento sono in formato PDF, scaricabili e quindi consultabili anche successivamente.

Per coloro che desiderano avere una consulenza personalizzata, si informa che, presso EMOSERVIZI sono avviati contatti con apposite società di consulenza in materia; per informazioni al riguardo telefonare al 02/69016918.

Segreteria AVIS Nazionale