

Associazione Dianova Onlus

Viale Forlanini, 121

20024 Garbagnate Milanese (MI)

e-mail di riferimento: dianova.onlus@dianova.it

Partita I.V.A.: 01824880023

Legale Rappresentante: Sig. Mauro Luccardini

Anno 2010



Documento Programmatico sulla Sicurezza (D.P.S.)

[Art. 6 Regolamento sulle misure minime di sicurezza - D.P.R. 28 Luglio 1999, n. 318, ripreso e integrato dalla Legge 196 del 30.06.2003 (Codice sulla privacy)]

Ruolo/Responsabilità	Nominativo	Firma
Legale rappresentante/Titolare dei dati	Mauro Luccardini	<i>Mauro Luccardini</i>
Responsabile del trattamento dei dati	Angelo Nazzari	<i>Angelo Nazzari</i>
Responsabile del trattamento dei dati	Simoes Perez Milagros	<i>Simoes Perez Milagros</i>
Responsabile del trattamento dei dati	Ombretta Garavaglia	<i>Ombretta Garavaglia</i>
Responsabile del trattamento dei dati	Fulvia Paggi	<i>Fulvia Paggi</i>
Responsabile del trattamento dei dati	Pasquale Landi	<i>Pasquale Landi</i>
Responsabile del trattamento dei dati	Rui Cardoso	<i>Rui Cardoso</i>
Responsabile del trattamento dei dati	Mauro Faggion	<i>Mauro Faggion</i>
Responsabile del trattamento dei dati	Giovanni Carrino	<i>Giovanni Carrino</i>
Responsabile del trattamento dei dati	Massimo Bagnaschi	<i>Massimo Bagnaschi</i>
Responsabile del trattamento dei dati	Pasquale Cicirelli	<i>Pasquale Cicirelli</i>
Responsabile del trattamento dei dati	Chon Perez	<i>Chon Perez</i>
Responsabile del trattamento dei dati	Sara Cecchetti	<i>Sara Cecchetti</i>
Responsabile del trattamento dei dati	Sara Scherillo	<i>Sara Scherillo</i>
Responsabile del trattamento dei dati	Vincenzo Contristano	<i>Vincenzo Contristano</i>
Responsabile del trattamento dei dati	Mario Espa	<i>Mario Espa</i>

Illegale un'attività di firma x

Garbagnate Milanese, li 25/02/2010.....

SI RICHIEDE LA POSIZIONE DEL TIMBRO POSTALE PER DATA CERTA

1 DOCUMENTO UNICO FORMATO DA N° 21 PAGINE
 25/03/2010 *[Signature]*

SCOPO E AMBITO DI APPLICAZIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Indice

Introduzione

L'analisi dei rischi

- Premessa
- Elenco dei rischi
- Cifratura dei dati relativi allo stato di salute

Le risorse umane per il trattamento dei dati:

- Premessa
- Titolare dei dati
- Responsabili del trattamento dei dati
- Incaricati del trattamento dei dati
- Amministratori di sistema
- Custode delle credenziali di autenticazione
- Altre risorse umane

La formazione del personale

Le misure di sicurezza e il controllo dell'accesso ai locali:

- Copie periodiche di backup
- Protezione da virus informatici o intrusioni non autorizzate nella rete informatica
- Sistema di autenticazione informatica
- Controllo dell'accesso ai locali
- Altre misure

Criteri di ripristino dei dati danneggiati

Descrizione dei documenti/moduli adottati

- Elenco lettere di incarico
- Elenco altri documenti/moduli

Conclusioni

Mario Furteradi

Introduzione

Il presente Documento Programmatico sulla Sicurezza dei dati è stato adottato, ai sensi delle disposizioni di cui all'Art. 34 del D. Lgs. 30 Giugno 2003, n. 196 (e relativo Allegato B), per definire le politiche di sicurezza in materia di trattamento di dati personali nonché i criteri tecnico-organizzativi adottati dall'emittente per la loro attuazione; il documento fornisce inoltre informazioni relative alla tipologia di dati personali sensibili trattati e all'analisi dei rischi connessi all'utilizzo degli strumenti mediante i quali viene effettuato il trattamento.

Le suddette politiche vengono adottate in tutte le sedi (legale/amministrativa e operative, dalle comunità terapeutiche ai centri di ascolto) in cui opera l'**Associazione Dianova Onlus**.

Il documento programmatico sulla sicurezza è stato riemesso per l'Anno 2010 da questa Associazione (Organizzazione non lucrativa di utilità sociale - Onlus) in ragione del trattamento dei dati di cui agli Artt. 22 e 24 della Legge 31 Dicembre 1996, n. 675 mediante gli elaboratori di cui all'Art. 3, comma 1, lettera b) del Regolamento di cui al D.P.R. sopra citato ed in ragione del successivo Codice sulla privacy e delle indicazioni dell'Ufficio del Garante.

AAA: le variazioni rispetto al documento precedente sono riportate in (grassetto + corsivo).

I dati personali possono essere "comuni" ovvero "sensibili"; l'elenco di questi ultimi è riportato seguito:

Dati sensibili trattati

Origini razziali e/o etniche
Convinzioni religiose, filosofiche o di altro genere
Opinioni politiche
Adesione a partiti/sindacati/associazioni/organizzazioni a carattere religioso/filosofico/politico/sindacale
Stato di salute
Vita sessuale

Plus
 per rivedere

Dati relativi ai provvedimenti di cui all'Art. 686 del Codice di Procedura Penale, commi 1, lettere a) e d), 2 e 3: dati giudiziari trattati

Dati evincibili dalle iscrizioni nel casellario giudiziario:
<input type="checkbox"/> condanna penale, <input type="checkbox"/> dichiarazione di abitudine del reato, <input type="checkbox"/> pene accessorie, ...

I documenti/moduli cui si rinvia nel presente documento costituiscono parte integrante del Documento Programmatico sulla Sicurezza dei dati dell'**Associazione Dianova Onlus**.

Si segnala sin d'ora che, nel presente documento e nei documenti/moduli di cui sopra, i termini trattamento, dato personale, dati identificativi, dati sensibili, dati giudiziari, titolare dei dati, responsabile del trattamento dei dati, incaricato del trattamento dei dati, interessato, diffusione, banca-dati e tutti gli altri termini ivi utilizzati vengono usati in conformità alle definizioni elencate

all'Art. 4 del D. Lgs. 30 Giugno 2003, n. 196.

In dettaglio, il Documento Programmatico sulla Sicurezza dei dati fornisce informazioni relative a:

- l'elenco dei trattamenti di dati personali decisi e attivati;
- la distribuzione di compiti/responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché le procedure da seguire per controllare l'accesso ai locali nei quali vengono conservati i dati personali oggetto del trattamento o l'accesso ai medesimi per via telematica;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento, garantendone la disponibilità in tempi "certi", comunque compatibili con i diritti degli interessati;
- la predisposizione di un piano di formazione per rendere edotti gli incaricati del trattamento dei dati in merito ai rischi che incombono sui dati e dei modi per prevenire i danni, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare dei dati o sull'introduzione di nuovi strumenti utilizzati per il trattamento dei dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura ovvero per la separazione di tali dati dagli altri dati personali dell'interessato (d'obbligo per gli organismi sanitari e gli esercenti le professioni sanitarie).

*Mano
p. 20/20/20*

In ragione dei suoi contenuti, il Documento Programmatico sulla Sicurezza dei dati deve essere divulgato e illustrato a tutti gli incaricati nominati con apposite lettere di incarico citate e descritte nel presente documento.

Il presente documento è valido per un anno: trascorso tale termine, e non oltre il 31 Marzo di ogni anno, esso sarà oggetto di opportune revisioni, per adeguarlo ad eventuali modifiche delle normative vigenti, al mutato livello di rischio cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o, in generale, ad un mutato assetto organizzativo.

L'analisi dei rischi

Premessa

L'analisi dei rischi ai quali sono soggetti i dati trattati vengono dettagliati in apposito documento (vedere **Modello A110**).

In tale documento viene riportata apposita lista dei rischi incombenti sui dati derivanti dal sistema di elaborazione, dal sistema operativo e dai programmi applicativi.

Nello stesso documento sono inoltre proposte le azioni correttive ovvero preventive da intraprendere.

L'analisi dei rischi è stata/viene e sarà redatta in relazione al progresso tecnologico; alla sostituzione, integrazione e/o sostituzione di hardware; agli aggiornamenti o alla sostituzione di sistemi operativi e/o programmi applicativi.

Per definire il piano richiesto dal Documento Programmatico sulla Sicurezza dei dati è stata riefettuata, anche quest'anno, la suddetta analisi, che ha comportato:

- la rilevazione dei rischi che gli strumenti utilizzati, i supporti cartacei e magnetici, i contenitori e gli archivi, le risorse umane, ...coinvolti/e nelle operazioni di trattamento dei dati personali possono correre
- l'individuazione delle minacce che possono causare tali rischi
- la valutazione delle conseguenze potenziali e la valutazione della loro gravità in tutti i casi in cui uno o più rischi si verificano

Prima fase

Elenco dei rischi

La prima definizione del piano/i suoi aggiornamenti annuali (questo compreso) si è basata/si basa/si baseranno sull'analisi dei seguenti rischi, minacce e conseguenze e sulla compilazione/revisione delle tabelle di cui alle pagine seguenti, anch'esse potenzialmente variabili nel tempo.

Rischi:

- distruzione o perdita, anche accidentale, di dati
- accessi non autorizzati
- trattamenti non consentiti o non conformi alle finalità della raccolta dei dati

Minacce:

- alterazione di dati, disastri naturali, quali incendi e/o allagamenti
- divulgazione/comunicazione non consentita/autorizzata
- duplicazione e diffusione di dati a scopo di lucro e/o di documento
- sottrazione/furto di dati, guasti delle apparecchiature informatiche

- errori umani causati da imperizia

Conseguenze:

- sanzioni di natura penale
- risarcimenti in sede civile
- sanzioni amministrative da parte del Garante
- perdite economico/finanziarie
- blocco dell'attività
- perdita di immagine
- costi gestionali
- responsabilità contrattuali

Cifratura dei dati relativi allo stato di salute

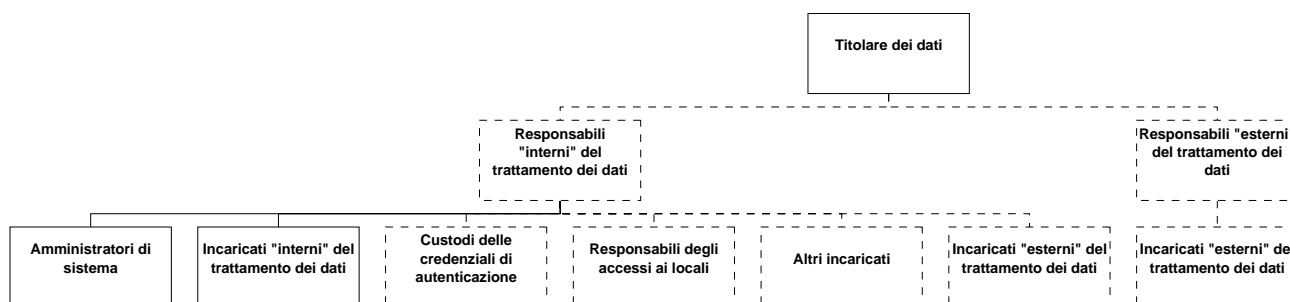
Qualora la tipologia dei dati trattati comprendesse anche quelli di tipo sanitario relativi allo stato di salute o alla vita sessuale, in apposito documento (vedere **Modello A080**) sono previste le misure idonee per gestire la separazione dei dati dall'individuazione diretta dell'interessato ed individuare i casi in cui possa necessitare la loro cifratura.

Maria Piera

Le risorse umane per il trattamento dei dati

Premessa

L'Associazione Dianova Onlus presenta il seguente organigramma per il trattamento dei dati:



Titolare dei dati

Al titolare dei dati spetta l'onere di individuare e incaricare uno o più responsabili del trattamento dei dati, qualora lo ritenesse opportuno.

La nomina deve avvenire per iscritto e, sempre per iscritto, il titolare deve elencare in dettaglio le mansioni assegnate.

Il titolare dei dati, a tal proposito, ha redatto/redige/redigerà apposite lettere di incarico da sottoscrivere per accettazione da parte di ogni responsabile del trattamento dei dati.

È cura del titolare dei dati conservare in luogo sicuro una copia delle lettere di incarico e istruire adeguatamente i suddetti responsabili in merito agli incarichi assegnati.

Nota: tra i compiti non delegabili assegnati al titolare dei dati è prevista la vigilanza sul rispetto da parte dei suddetti responsabili degli incarichi loro assegnati, nonché sulla diligente osservanza delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riguardo alle misure di sicurezza da adottare.

Nota: nel caso in cui non venisse nominato alcun responsabile del trattamento dei dati, il titolare dei dati ne assume il ruolo e tutte le responsabilità.

Tra i compiti istituzionali del titolare dei dati rientra l'impegno a provvedere, direttamente o per delega, ad agevolare l'accesso ai dati personali da parte dell'interessato, a fornirgli le informazioni richieste e a contenere al meglio i tempi per il riscontro del richiedente.

Responsabili del trattamento dei dati

In ottemperanza all'Art. 29 del D. Lgs. 30 Giugno 2003, n. 196, il titolare dei dati, come sopra accennato, può nominare uno o più responsabili del trattamento dei dati con apposita lettera di incarico (vedere **Modello C010**), riportandone gli estremi in un verbale di consiglio.

I suddetti responsabili devono essere individuati fra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riguardo alla loro sicurezza.

I suddetti responsabili, pertanto, dovranno adottare tutte le misure idonee ad assicurare l'integrità

Maria Furci

dei dati oggetto del trattamento, a ridurre i rischi di diffusione o di trattamento di dati non consentiti e a mantenere in piena efficienza tutti gli strumenti e la struttura organizzativa dell'**Associazione Dianova Onlus**, al fine di perseguire gli scopi dettati dal presente Documento Programmatico sulla Sicurezza dei dati.

Per esigenze organizzative, il titolare dei dati può suddividere i compiti fra i diversi responsabili del trattamento dei dati nominati.

Questi ultimi hanno il dovere istituzionale di informare tempestivamente il titolare dei dati di eventuali incidenti o della sopravvenuta mancanza dei requisiti minimi di sicurezza richiesti.

Ai singoli responsabili del trattamento dei dati è affidato anche il compito di redigere e di aggiornare l'elenco dei trattamenti effettuati sui dati personali (vedere **Modello A055**).

Ai suddetti responsabili viene inoltre conferita la possibilità di nominare uno o più incaricati del trattamento dei dati e di istruirli adeguatamente per renderli idonei a svolgere le mansioni loro assegnate.

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C010**), la nomina dei suddetti responsabili si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

Ai fini della dovuta formalizzazione e di una reciproca conoscenza delle mansioni di competenza ai sensi del Codice sulla *privacy*, si riportano nel seguito le mansioni del titolare dei dati, delegate al suo Legale Rappresentante e quelle dei responsabili del trattamento dei dati.

Mansioni primarie del Legale Rappresentante del titolare dei dati:

- definisce le finalità del trattamento dei dati
- nomina i responsabili del trattamento dei dati
- effettua e sottoscrive le *eventuali* Notificazioni al Garante
- stabilisce per iscritto, in accordo con i responsabili "nominati" del trattamento dei dati, le modalità di raccolta, accesso e delle altre forme di trattamento dei dati personali
- vigila costantemente - direttamente o per delega scritta - sull'osservanza delle misure decise autonomamente e/o in accordo con i responsabili "nominati" del trattamento dei dati, anche per il tramite di monitoraggi periodici

Mansioni primarie dei responsabili del trattamento dei dati:

- stabilisce per iscritto, in accordo con il Legale Rappresentante del titolare dei dati, le modalità di raccolta, accesso e delle altre forme di trattamento dei dati personali
- fornisce per iscritto queste ultime agli incaricati del trattamento dei dati (oltre alle modalità/opportunità di accesso, ove del caso) nei limiti di deleghe assegnate per iscritto
- vigila costantemente sull'osservanza di tali misure
- effettua periodicamente un adeguato monitoraggio del flusso di tutti i dati trattati

Musio
Purcellini

- stabilisce, nelle more, e rende operanti dopo l'emissione dei relativi regolamenti e dei successivi aggiornamenti, tutte le misure di sicurezza dei dati ufficialmente emesse dal Garante
- verbalizza i principali momenti di monitoraggio, a fini storici e di soddisfacimento di eventuali specifiche richieste del Garante

Incaricati del trattamento dei dati

Qualora la gestione delle banche-dati richieda l'intervento operativo di altri soggetti, il titolare dei dati ovvero i responsabili del trattamento dei dati possono nominare uno o più incaricati del trattamento dei dati con apposita comunicazione/nomina scritta (vedere **Modello C020**).

Sempre per iscritto devono essere specificati i compiti loro assegnati.

Questa lettera di incarico deve essere sottoscritta dal soggetto incaricato e sarà cura di chi ha conferito l'incarico custodire copia della nomina in luogo sicuro.

Compito degli incaricati del trattamento dei dati è quello di svolgere gli incarichi loro assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente Documento Programmatico sulla Sicurezza dei dati.

In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti minimi di sicurezza, i suddetti incaricati debbono comunicare tempestivamente tale circostanza al responsabile del trattamento dei dati ovvero, mancando quest'ultimo, al titolare dei dati.

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C020**), la nomina dei suddetti incaricati si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

Amministratori di sistema

Ogni responsabile del trattamento dei dati ovvero il titolare dei dati conferiscono a uno o più incaricati le mansioni di gestione delle soluzioni informatiche sia hardware sia software adottate per la gestione e la tenuta in sicurezza delle banche-dati.

La nomina avviene per iscritto e nella lettera di incarico (vedere **Modello C030**) vengono dettagliati i compiti assegnati, compreso quello di approntare i mezzi necessari per effettuare le copie di sicurezza dei dati richieste dal D. Lgs. 30 Giugno 2003, n. 196 ed il loro ripristino in caso di accidentale distruzione.

L'amministratore di sistema ha anche l'onere di valutare periodicamente lo stato di efficienza delle soluzioni informatiche adottate e di provvedere alla loro modifica o integrazione in base all'esperienza acquisita ed al progresso tecnologico.

Qualora non fosse già stato incaricato un altro soggetto, l'amministratore di sistema può anche essere nominato custode delle credenziali di autenticazione (vale a dire: codici identificativi, User ID, password, ecc.) assegnate ad ogni soggetto incaricato del trattamento dei dati.

L'amministratore di sistema, nello svolgere questo incarico, si deve attenere a quanto previsto nel presente Documento Programmatico sulla Sicurezza dei dati per il custode delle credenziali di

Maria Teresa

autenticazione (vedere nel seguito).

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C030**), la nomina dei suddetti amministratori si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

Nota: nel caso in cui non venga nominato alcun amministratore di sistema, le relative mansioni vengono svolte dal responsabile del trattamento dei dati o, in sua mancanza, dal titolare dei dati.

Custode delle credenziali di autenticazione

Il responsabile del trattamento dei dati, di concerto con il titolare dei dati, può nominare uno o più custodi delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati.

L'incarico viene assegnato per iscritto e la lettera (vedere **Modello C040**) deve essere conservata in un luogo sicuro da parte del responsabile del trattamento dei dati.

Il custode delle credenziali di autenticazione sottoscrive apposito documento (vedere **Modello A030**) con il quale prende visione di tutte le credenziali di accesso da custodire.

Le credenziali non dovranno essere divulgate e dovranno essere custodite in luogo sicuro.

Spetta al suddetto custode definire le modalità di utilizzo delle credenziali di autenticazione in caso di impedimenti o di prolungata assenza dell'incaricato del trattamento dei dati ai quali siano state assegnate, nel rispetto di un sistema di autorizzazione e dei criteri di assegnazione delle password degli incaricati (vedere **Modelli A050 e A060**).

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C040**), la nomina dei suddetti custodi si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

Nota: in mancanza di un custode delle credenziali di autenticazione, le mansioni sopra riportate saranno svolte dall'amministratore del sistema o, in sua mancanza, dal soggetto che ha conferito l'incarico (responsabile del trattamento dei dati).

Altre risorse umane

Ove lo si ritenga necessario, si provvede alla:

- Nomina del responsabile degli accessi ai locali (vedere **Modello C050**)

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C050**), la nomina dei suddetti responsabili si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

- Nomina del responsabile "esterno" del trattamento dei dati (con assegnazione delle mansioni) (da redigere solo all'occorrenza) (vedere **Modello C060**)

Nota: se non diversamente previsto nella lettera di incarico (vedere **Modello C060**), la nomina dei suddetti responsabili si intende a tempo indeterminato e decade o per dimissioni ovvero per revoca comunicata per iscritto (o con idonei mezzi informatici) dal titolare dei dati.

- Nomine per altri incarichi (da redigere solo all'occorrenza). (vedere **Modello C070**)

Qualora il trattamento dei dati venisse affidato in parte o in toto a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico.

Plus personal

Sarà cura del titolare dei dati conservare in luogo sicuro copia di tale lettera.

La scelta dei responsabili del trattamento dati “esterni” deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti dal D. Lgs. 30 Giugno 2003, n. 196.

Sarà poi compito del responsabile del trattamento dei dati “esterno” nominare i propri incaricati del trattamento dei dati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.

Ogni trattamento di dati affidato a terzi verrà elencato su apposito documento (vedere **Modello A020**), in cui viene tra l’altro riportato l’elenco delle sedi e uffici nelle/nei quali avviene il trattamento dei dati), omologamente di quanto avviene per la struttura qui in esame (vedere **Modello A010**).

Nello stesso documento dovranno essere riportati anche i luoghi dove vengono fisicamente trattati e conservati i dati.

Al titolare dei dati spetta il compito di vigilare sull’operato del responsabile del trattamento dei dati “esterno” affinché non vengano mai meno le misure minime di sicurezza dei dati.

Maria
Purcellini

La formazione del personale

Al responsabile del trattamento dei dati o, in sua mancanza, al titolare dei dati spetta il compito di provvedere all'opportuna formazione di tutti gli incaricati del trattamento dei dati al fine di:

- garantire il massimo rispetto delle procedure elencate nel presente Documento Programmatico sulla Sicurezza dei dati
- rendere edotto il personale sui rischi che incombono sui dati
- informare il personale sulle responsabilità che ne derivano

Il responsabile del trattamento dei dati o, in sua mancanza, il titolare dei dati valuta opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.

Il responsabile del trattamento dei dati o, in sua mancanza, il titolare dei dati, provvede a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico e/o al cambiamento di mansioni.

I piani di formazione, prodotti annualmente, sono dettagliati in apposito documento (vedere **Modello A040**).

Oltre alla formazione specifica delle mansioni, programmata e realizzata con periodicità annuale, l'**Associazione Dianova Onlus** ha prodotto due "regole d'oro", divulgate a tutto il proprio personale:

- Istruzioni sulle modalità di trattamento dei dati personali su supporti cartacei
 - Istruzioni sulle modalità di trattamento di dati personali su supporti informatizzati/elettronici, ...
- ... qui riportate nelle pagine seguenti, cui si rinvia.

Flavia Perreoli

Istruzioni sulle modalità di trattamento dei dati personali su supporti cartacei

L'accesso ai contenuti di tutti i supporti cartacei sopra citati da parte di ogni incaricato del trattamento dei dati deve essere effettuato per le sole finalità di cui alle mansioni specifiche di ogni incaricato (che si evincono dagli specifici verbali di nomina (vedere **Modello C020**).

L'utilizzo del supporto cartaceo è regolato come segue:

- a) prelievo al momento dell'utilizzo dall'archivio (personale o comune) da parte dell'incaricato
- b) eventuale concessione da parte del primo incaricato dell'utilizzo dello stesso supporto cartaceo ad altri incaricati di cui egli conosca adeguatamente la mansione; in caso contrario - e solo in caso contrario - viene fatto obbligo al primo incaricato di richiedere all'altro incaricato richiesta scritta firmata e datata di consultazione estemporanea del supporto cartaceo, approvata e datata dal primo incaricato o da un suo superiore o, ancora, dal responsabile del trattamento dei dati (*ove presente*) (questa richiesta scritta sarà conservata dal primo incaricato); la responsabilità per eventuali consegne e/o successive comunicazioni/diffusioni illecite viene attribuita al primo incaricato solo e solo se l'approvazione sia stata oggettivamente fornita a chi non ne abbia diritto e ciò risulti dall'approvazione scritta firmata dallo stesso primo incaricato
- c) utilizzo del supporto nei termini temporali oggettivamente necessari e sufficienti alla bisogna
- d) archiviazione al termine dell'utilizzo a cura del primo incaricato

Nota 1: ogni incaricato deve avere adeguata cura del proprio archivio personale (avendolo!), regolandosi come segue:

- i contenitori (cassetti, cassettiere, armadi, armadi speciali, ecc. debbono risultare chiusi, in presenza di chiavi concesse dalla struttura, in caso di assenza dell'incaricato)
- le rispettive chiavi (*ove presenti*) debbono essere conservate dall'incaricato o rese in futuro - se possibile - disponibili in apposita postazione ad accesso controllato
- i supporti cartacei contenenti dati personali debbono essere riposti dall'incaricato nei rispettivi contenitori anche in caso di sua assenza temporanea (questa regola vale anche per agende ed elenchi telefonici privati)

Muro per archivi

Nota 2:

L'accesso agli archivi comuni "potrebbe" essere regolato rendendo disponibili chiavi di accesso con rilascio da parte di uno solo degli incaricati (= incaricato "super partes"); le aree dell'archivio comune "dovrebbero" essere ben separate per tipologia di dati conservati (personali sensibili, giudiziari, comuni) ...ma questa scelta è "opzionale"

L'entrata all'archivio comune "dovrebbe" risultare chiusa in caso di assenza del citato incaricato "super partes"

Nota 3: L'eventuale trasmissione di dati presenti su supporti cartacei richiesta per iscritto da un altro incaricato deve essere effettuata, quando non lo sia direttamente *brevi manu* dal primo incaricato, per il tramite di busta sigillata, con sigla o firma ed eventuale timbro del mittente (= primo incaricato), con l'evidenza precisa del destinatario e con l'avvertenza di avvisare quest'ultimo da parte del primo incaricato - se l'impegno non risulta oneroso - della trasmissione in corso

Nota 4: I supporti cartacei obsoleti debbono essere distrutti - fruendo di appositi distruggi-documenti, *ove presenti* - dall'incaricato la cui mansione prevede la loro conservazione sino al momento dell'obsolescenza o, in alternativa, resi disponibili in appositi contenitori per un loro successivo inoltro a macero (= aree di segregazione e/o di distruzione); eventuali dubbi sull'opportunità o meno della distruzione saranno sottoposti per una decisione incontrovertibile al titolare dei dati o al responsabile del trattamento dei dati (*ove presente*)

Istruzioni sulle modalità di trattamento di dati personali su supporti informatizzati/elettronici

L'accesso ai contenuti da parte di ogni incaricato del trattamento dei dati deve essere effettuato per le sole finalità di cui alle sue mansioni, quindi entro i limiti assegnati inizialmente ad ogni incaricato nella fase di definizione del suo profilo di accesso agli archivi meccanografici; in altre parole: ogni incaricato continuerà a poter/dover accedere ai dati cui normalmente accede per svolgere la propria attività lavorativa

L'utilizzo del supporto informatizzato deve essere regolato come segue:

- a) accesso per il tramite della propria password (qualora gli sia stata assegnata) al momento dell'utilizzo dell'archivio da parte dell'incaricato
- b) eventuale concessione da parte del primo incaricato dell'utilizzo dello stesso supporto meccanografico ad altri incaricati di cui egli conosca adeguatamente la mansione; in caso
- c) contrario viene fatto obbligo al primo incaricato di richiedere all'altro richiesta scritta firmata e datata di consultazione estemporanea del supporto meccanografico, approvata e datata dal primo incaricato (si rammenti che è sufficiente questo livello di approvazione!) o da un suo superiore o, ancora, dal responsabile del trattamento dei dati (*ove presente*) (AAA: questa richiesta sarà conservata dal primo incaricato); la responsabilità per eventuali successive comunicazioni/diffusioni illecite viene attribuita al primo incaricato solo e solo se l'approvazione sarà stata fornita a chi non ne abbia diritto e ciò risulti dall'approvazione scritta firmata dallo stesso primo incaricato
- d) utilizzo del supporto meccanografico nei termini temporali oggettivamente necessari e sufficienti alla bisogna
- e) chiusura tempestiva della sessione, al termine dell'utilizzo, a cura del primo incaricato

Note:

Ogni incaricato deve avere adeguata cura di ogni archivio meccanografico cui ha accesso:

il video-terminale o il personal computer o, ancora, il terminale di collegamento a reti esterne possono essere dotati di screen-saver o di sistemi di ibernazione o, ancora, di sistemi di rilascio automatico della connessione; qualora ciò non sia stato previsto dalla struttura, in caso di allontanamento, anche temporaneo, l'incaricato deve preventivamente chiudere la sessione: questa norma "deve" essere introdotta per uniformarsi alle Leggi sulla *privacy* già introdotte in altri Paesi della UE; identico accorgimento deve essere preso al termine dell'attività lavorativa giornaliera: vale la stessa nota sulla norma.

I supporti meccanografici obsoleti debbono essere distrutti - fruendo, se presente, dell'apposito sistema di cancellazione in dotazione - dall'incaricato la cui mansione prevede la loro conservazione sino al momento dell'obsolescenza o, su specifica richiesta dell'incaricato, da personale esperto di informatica.

I supporti meccanografici obsoleti comuni saranno invece distrutti ad esclusiva cura di esperti di informatica, secondo piani di cancellazione predisposti o comunque previsti, annualmente approvati anche dal titolare dei dati o dal responsabile del trattamento dei dati (*ove presente*); eventuali dubbi sull'opportunità o meno della distruzione saranno sottoposti per una decisione incontrovertibile al titolare dei dati (e ciò potrà essere richiesto ogni volta che sussistano dubbi in proposito!)

*Plan
presented*

Le misure di sicurezza e il controllo dell'accesso ai locali

In ottemperanza al D. Lgs. 30 Giugno 2003, n. 196, il presente Documento Programmatico sulla Sicurezza dei dati prevede l'organizzazione e l'introduzione di idonee misure di sicurezza da adottare, volte a garantire la sicurezza dei dati.

Essa si esplica nella loro diligente custodia, al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.

Il responsabile del trattamento dei dati o, in sua mancanza, il titolare dei dati appronteranno tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnologico.

Sono state previste specifiche misure di sicurezza sia per quanto riguarda la custodia di archivi elettronici e non, sia l'accesso ai locali ove i dati oggetto del trattamento sono fisicamente conservati.

La procedura di preservazione dal rischio di perdita dei dati trattati con mezzi informatici o dalla divulgazione non autorizzata si esplica nella previsione di un piano basato su:

Copie periodiche di Backup

Tale procedura, che il responsabile del trattamento dei dati ovvero il titolare dei dati stilano di concerto con l'amministratore di sistema, deve fornire le istruzioni e le modalità in merito al tipo di supporto utilizzato, all'impiego di specifici software per l'esecuzione controllata di salvataggi automatizzati, alla nomina degli incaricati del trattamento dei dati che eseguiranno le copie di Backup, alla custodia dei supporti nei quali sono stati memorizzati i dati, alla distruzione dei supporti dopo un certo lasso di tempo o, comunque, alla cancellazione dei dati dai supporti di Backup in maniera tale da impedirne ogni possibile consultazione.

La procedura di salvataggio prevede anche il monitoraggio di tutte le operazioni di merito, affinché il responsabile del trattamento dei dati ovvero il titolare dei dati possano individuare periodicamente circostanze che impongano l'adozione di un diverso piano di Backup o il suo aggiornamento.

Il salvataggio dei dati dovrà avvenire con cadenza almeno settimanale.

Questa procedura di backup e ripristino dati è dettagliata in apposito documento (vedere **Modello A100**) e viene resa nota a tutti gli incaricati del Backup a cura dell'amministratore di sistema.

Protezione da virus informatici o intrusioni non autorizzate nella rete informatica

Il responsabile del trattamento dei dati ovvero il titolare dei dati incaricano l'amministratore di sistema di approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da Virus informatici o da intrusioni non autorizzate nel sistema medesimo.

L'amministratore di sistema provvede a dettagliare in apposito documento (vedere **Modello A90**) tutte le misure adottate, compresi l'utilizzo di appositi programmi Antivirus, Firewall e qualsiasi

Maria Pierluigi

ulteriore soluzione informatica che ritenga opportuna per diminuire la vulnerabilità del sistema.

È anche compito dell'amministratore di sistema pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione delle case produttrici di software per correggere i difetti dei programmi o dei sistemi operativi utilizzati.

L'amministratore di sistema può prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal D. Lgs. 30 Giugno 2003, n. 196.

Tutte le misure di sicurezza previste dall'amministratore di sistema debbono essere periodicamente valutate per adattare la procedura all'evoluzione tecnologica.

L'amministratore di sistema deve inoltre provvedere ad istruire adeguatamente eventuali incaricati al trattamento dei dati e consegnare loro copia del **Modello A90** (elenco programmi adottati per la sicurezza dei dati trattati con strumenti elettronici, ovvero elenco programmi antivirus).

In caso di infezione del sistema da parte di Virus informatici, l'amministratore di sistema deve infine adottare tempestivamente tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; egli deve quindi individuare le cause di tale infezione e provvedere a rimuoverle.

Sistema di autenticazione informatica

Così come previsto dall'Allegato B al D. Lgs. 30 Giugno 2003, n. 196, il trattamento dei dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione.

Il responsabile del trattamento dei dati o, in sua mancanza, il titolare dei dati, in accordo con gli amministratori di sistema, definisce le modalità di assegnazione delle credenziali di autenticazione agli incaricati del trattamento dei dati.

Le credenziali possono consistere nell'assegnazione di User ID e password ovvero nell'utilizzo di dispositivi associati ad un codice identificativo o anche ad una caratteristica biometrica.

Ad ogni soggetto autorizzato all'accesso alle banche-dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche-dati gestite.

Nota: se fra le credenziali è prevista l'assegnazione di una password, questa non deve essere di lunghezza inferiore agli otto caratteri (o al numero massimo possibile se lo strumento elettronico utilizzato non lo consente) di tipo almeno alfanumerico.

Al primo utilizzo della password, l'incaricato provvederà a modificarla e, successivamente, la modificherà periodicamente con cadenza almeno semestrale, a meno che la banca dati non contenga dati personali sensibili; in quest'ultimo caso la parola chiave andrà modificata almeno ogni tre mesi. Ogni persona incaricata del trattamento dei dati deve adottare tutte le cautele possibili per garantire la segretezza delle credenziali di autenticazione assegnate.

Maria Perrella

Controllo dell'accesso ai locali

Per ciò che concerne la gestione dei dati non trattati con strumenti elettronici, sono appositamente definite la modalità di trattamento e i vari supporti utilizzati.

Vengono altresì definite tutte le misure di sicurezza da adottare per evitare l'accidentale perdita o il danneggiamento dei dati.

Tutte le modalità di trattamento dati senza l'ausilio di strumenti elettronici e della loro sicurezza sono dettagliate in apposito documento (vedere **Modello A120**).

Nota: il Libro-soci, il Libro-matricola, ogni Registro-presenze, il Registro-infortuni e le Certificazioni mediche sono supporti cartacei di dati personali "comuni" e "sensibili" e, come tali, richiedono di essere trattati con le modalità predisposte in merito dall'**Associazione Dianova Onlus**.

Questo modello contiene le modalità di accesso ai locali dove fisicamente vengono gestite le banche-dati, nel caso di dati trattati sia con l'ausilio di strumenti elettronici sia con altri strumenti.

È cura del responsabile del trattamento dei dati o, in sua mancanza, del titolare dei dati redigere tale documento.

In ogni caso è fatto divieto a chiunque di divulgare informazioni concernenti i dati oggetto del trattamento, effettuarne copie di qualsiasi natura (su supporti cartacei, informatici, audiovisivi, ecc.) e distruggere, sottrarre o manipolare il contenuto delle banche-dati se non espressamente autorizzato dal responsabile del trattamento dei dati o dal titolare dei dati.

Note integrative su:

- La gestione dei curriculum: all'atto del ricevimento (via fax, busta, *brevi manu* o via e-mail), qualora non debbano essere "trattati" al momento, i curriculum debbono essere classificati e riposti in armadi chiusi, la cui chiave sia detenuta soltanto da persona delegata formalmente; il trattamento avrà inizio nella fase istruttoria di ogni processo di preselezione e comporterà, all'atto del primo e/o unico colloquio, la preventiva sottomissione al candidato dell'informativa appositamente predisposta; l'intervista potrà avere inizio soltanto dopo l'apposizione da parte del candidato della data e della firma nei campi appositi di detta informativa e la restituzione di detta copia all'intervistatore; è fatto inoltre obbligo alle persone delegate formalmente di analizzare con frequenza non superiore all'anno solare i curriculum residui, provvedendo alla loro eliminazione fisica nel caso in cui risultino essere oggettivamente obsoleti
- Le certificazioni mediche: esse debbono essere prodotte sempre in busta chiusa e debbono evidenziare l'indicazione del destinatario, sia che siano consegnate *brevi manu* a chiunque all'interno della struttura, sia che siano spedite, sia che siano consegnate *brevi manu* alla persona delegata

Altre misure

L'**Associazione Dianova Onlus** ha formalizzato le modalità di protezione dei dati (vedere **Modello A70**) e introdotte ulteriori misure in caso di trattamento di dati sensibili o giudiziari (vedere **Modello A80**).

Nota formale

Criteria di ripristino dei dati danneggiati

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, ogni incaricato, di concerto con l'amministratore di sistema, provvederà a ripristinare i dati mediante utilizzo delle copie di Backup realizzate in conformità a quanto descritto in apposito documento (vedere **Modello A100**).

L'amministratore di sistema può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, registrazioni audiovisive, ecc.) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici sia quelli trattati con altri tipi di strumenti.

In caso di distruzione o di danneggiamento degli strumenti utilizzati per l'accesso ai dati, l'amministratore di sistema (o, in sua mancanza, un incaricato nominato dal responsabile del trattamento dei dati ovvero dal titolare dei dati) provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.

Nota: la procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità al punto 23 dell'allegato B del D. Lgs. 30 Giugno 2003, n. 196.

Ad ogni evento che comporti distruzione, danneggiamento o problemi di accesso ai dati dovrà essere opportunamente aggiornata l'analisi dei rischi riportata nel presente Documento programmatico sulla Sicurezza dei dati.

Maria Perrotti

Descrizione dei documenti/moduli adottati

Elenco lettere di incarico

C010 – Lettera di incarico del responsabile del trattamento dei dati e mansioni assegnate (da Titolare dei dati ai Responsabili del trattamento dei dati)

C020 – Nomina dell'incaricato del trattamento dei dati e mansioni assegnate (da Titolare dei dati ovvero da Responsabile del trattamento dei dati agli Incaricati del trattamento dei dati)

C030 – Lettera di incarico dell'amministratore del sistema e mansioni assegnate (da Titolare dei dati ovvero da Responsabile del trattamento dei dati agli Amministratori di sistema)

C040 – Lettera di incarico al custode delle credenziali di autenticazione e mansioni assegnate (da Titolare dei dati ovvero da Responsabile del trattamento dei dati ai Custodi delle credenziali di autenticazione)

C050 – Nomina del responsabile degli accessi ai locali (da Titolare dei dati ovvero da Responsabile del trattamento dei dati ai Responsabili degli accessi ai locali)

C060 – Lettera di incarico del responsabile del trattamento dei dati "esterno" (e mansioni assegnate) (redatta solo all'occorrenza a firma del Titolare dei dati ovvero del Responsabile del trattamento dei dati)

C070 – Lettera di nomina di altri incarichi (redatta solo all'occorrenza a firma del Titolare dei dati ovvero del Responsabile del trattamento dei dati).

Maria Benedetti

Elenco altri documenti/moduli

Tutte le informative richieste dal D. Lgs. 30 Giugno 2003, n. 196

A010 – Elenco sedi ed uffici nei quali avviene il trattamento dei dati (comprensivo dei rispettivi responsabili)

A020 – Elenco sedi ed uffici nei quali avviene il trattamento dei dati affidato all'esterno della struttura del titolare (redatto solo all'occorrenza)

A030 – Elenco degli incaricati al trattamento dei dati personali, sottoscritto dai Custodi delle credenziali di autenticazione

A040 – Piano di formazione degli incaricati, approvato dal Titolare dei dati ovvero dal Responsabile del trattamento dei dati

A050 – Sistema di autorizzazione e criteri di assegnazione delle password degli incaricati, sottoscritto dagli Incaricati del trattamento dei dati

A055 – Elenco dei trattamenti di dati personali

A060 – Criteri di assegnazione delle password nei sistemi di elaborazione, sottoscritto dagli assegnatari

A070 – Modalità di protezione dei dati

A080 – Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

A090 – Elenco programmi adottati per la sicurezza dei dati trattati con strumenti elettronici

A100 – Procedura di backup e ripristino dati

A110 – Analisi dei rischi incombenti sui dati

A120 – Modalità di trattamento dei dati senza l'ausilio di strumenti elettronici.

Maria Perreoli

Conclusioni

Incontro di Febbraio 2010:

Partecipanti : Il personale di coordinamento.

Argomenti discussi:

Nel corso dell'incontro è stata erogata la formazione prevista dal D. Lgs. 196/03; il corso di aggiornamento è stato anche predisposto in formato cartaceo dal Consulente in materia, Dott. Ing. M. M. Massara, e sarà reso disponibile a tutto il personale.

Ai sensi delle indicazioni dell'Ufficio del Garante è stata inoltre predisposta la Tabella degli amministratori, *cui si rinvia*.

Contestualmente è stato rivisto il Documento Programmatico sulla Sicurezza (D.P.S.), di cui il presente verbale è parte integrante nella sua versione di revisione annuale per il 2010.

ASSOCIAZIONE DIANOVA ONLUS
C.P. 97033640158 - P. IVA 01824880023
sede legale e amministrativa
V.le Forlanini, 121 - 20024 Garbagnate Mil. (MI)
Tel. 02.99022033 - Fax 02.99022452
E-mail: contabile@dianova.it

Marco Perreoli