

ROTARY INTERNATIONAL

Protezione dei dati personali

D. Lgs 196/2003 - Privacy

Applicazioni in un Club di servizio

Quaderno di informazioni operative n° 5



TQM-RRVF
Total Quality Management
Rotarians Fellowship
Sezione Italiana

ROTARY INTERNATIONAL

Protezione dei dati personali

D. Lgs 196/2003 - Privacy

Applicazioni in un Club di servizio



Quaderno di informazioni operative n° 5

A cura di:

TQM-RRVF
Total Quality Management
Rotarians Fellowship
Sezione Italiana
Milano, Dicembre 2005

TQM-RRVF
Total Quality Management
Rotarians Fellowship
Sezione Italiana

ha già pubblicato

- Quaderno di informazioni operative
La qualità nei Club Rotary
- Quaderno di informazioni operative n°1
I principi della qualità
- Quaderno di informazioni operative n°2
La qualità nella formazione
- Quaderno di informazioni operative n°3
La qualità in sanità
- Quaderno di informazioni operative n°4
La qualità nel turismo per un turismo di qualità

Rotary International
Total Quality Management
Rotarians Fellowship
Sezione Italiana

© Copyright 2005

E' possibile utilizzare i contenuti di questo quaderno citando la fonte
Edizione fuori commercio



Indice

Introduzione	pag. 5
Codice in materia di protezione dati personali	pag. 7
Parte Prima	
1. Premessa	pag. 9
2. Riferimenti	pag. 10
3. Finalità	pag. 11
4. Definizioni	pag. 12
- Dato personale	pag. 13
- Banca dati	pag. 14
- Titolare del trattamento	pag. 14
- Responsabili del trattamento	pag. 14
- L'interessato	pag. 16
- Garante	pag. 17
- Comunicazione	pag. 17
- Diffusione	pag. 17
- Informativa	pag. 17
- Consenso	pag. 18
- Notifica al Garante	pag. 19
5. Misure di sicurezza (all. B al "Codice")	pag. 20
6. Documento Programmatico per la sicurezza (DPS)	pag. 21
Parte Seconda	
APPLICAZIONE del "CODICE" in un ROTARY CLUB	pag. 23
Parte Terza	
FAC-SIMILE - DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DEI DATI DPS	pag. 27
1. Scopo	pag. 27
2. Riferimenti	pag. 27
3. Definizioni e abbreviazioni	pag. 28
4. Dati personali	pag. 28
5. Trattamento	pag. 29
- Titolare, Responsabile, Incaricati	pag. 29
6. Elenco banche dati	pag. 30
7. Analisi dei rischi	pag. 30
8. Descrizione del sistema informatico	pag. 31
9. Misure fisiche di sicurezza	pag. 31
10. Misure logiche di sicurezza	pag. 32
11. Misure organizzative di sicurezza	pag. 33
12. Formazione degli incaricati	pag. 33
13. Controlli periodici	pag. 33
14. Aggiornamento del DPS	pag. 33



Indice (allegati)

Parte Quarta

Allegato 1

MISURE MINIME DI SICUREZZA

- Misure fisiche di sicurezza

- Misure logiche di sicurezza

- Misure organizzative di sicurezza

pag. 35

pag. 35

pag. 36

pag. 36

Allegato 2

FAC-SIMILE

INFORMATIVA E CONSENSO (attività istituzionali)

pag. 37

Allegato 3

FAC-SIMILE DI LETTERA DI INCARICO

pag. 39

Allegato 4

FAC-SIMILE

INFORMATIVA E CONSENSO PER DATI PERSONALI

NON COMUNI

pag. 41

APPENDICE

GUIDELINES FOR THE USE OF

ELECTRONIC COMMUNICATION IN

ROTARY INTERNATIONAL

pag. 43



Introduzione

La International Fellowship for Total Quality Management raggruppa un centinaio di Rotariani in tutto il mondo che si occupano di Qualità nei vari aspetti.

Nell'ambito della Azione Interna della attività rotariana e per dare una significativa risposta a quanti affacciandosi al mondo della qualità hanno dubbi e perplessità, dal 1998 si è costituita anche in Italia la sezione della

**Total Quality Management
Rotarians Fellowship
(TQM-RRVF)**

I Rotariani che fanno parte di questa Fellowship intendono quindi mettere a disposizione la propria esperienza professionale - in quanto soggetti cioè che hanno già affrontato tali problemi - per i colleghi che hanno dubbi e/o perplessità in merito.

Gli aderenti svolgono la propria attività professionale nei più svariati campi ed intendono dare il proprio contributo al fine di trasmettere le proprie esperienze acquisite ad altri Rotariani che vogliono affrontare tematiche simili.

Per maggiori informazioni riguardanti l'attività della Fellowship
è disponibile il sito internet

www.rotarytqm.it



Gli aderenti alla Fellowship sono Rotariani di varie parti d'Italia e agiscono esclusivamente su base volontaria nello spirito rotariano del servire.

Il quaderno predisposto, il sesto di una serie su tematiche varie, vuole essere un contributo alla attività previste dalla vigente legge che obbliga ogni soggetto che detiene a vario titolo elenchi di soggetti contenenti dati che vengono gestiti in forma elettronica e non ad alcuni adempimenti formali.

L'attività legata alla "Privacy" è in qualche modo riconducibile alla gestione di un Club "in qualità" ed è per questo che la TQM-RRVF offre questo contributo ad una gestione corretta della problematica relativa. Nello spirito del miglioramento continuo, ogni eventuale commento e/o suggerimento sarà apprezzato.

Per contattarci e-mail: rotarytqm@tiscali.it

I componenti della fellowship

Dicembre 2005 - Rev. 0 - emissione

Hanno contribuito alla realizzazione di questo studio
i componenti della Commissione:

Vittorio Cariatì
Stefano Farnè
Pietro Freschi
Paolo Grondona
Fabio Pasello
Antonio Todesco

R.C. Milano Sud-Est (D 2040)
R.C. Monza Nord Lissone (D 2040)
R.C. Milano Aquileia (D 2040)
R.C. Cantù (D 2040)
R.C. Rho Fiera Centenario (D 2040)
R.C. Legnago (D 2060)

Ai quali vanno sentiti ringraziamenti

Pietro C. Freschi
Coordinatore Italia TQM - RRVF



Codice in materia di protezione dei dati personali

D. Lgs. 196/2003

Alla nascita delle automobili è seguito il “Codice della Strada”, alla diffusione dei computer e di Internet fa ora seguito il “Codice della Privacy”.

Il presente documento vuole essere una traccia per l'applicazione del “Codice della Privacy” ai Club di servizio in generale ed ai Club Rotary in particolare.

Il quaderno si compone di quattro parti:

- la prima, è una descrizione generale dei requisiti richiesti dalla legge. Le definizioni ed i riferimenti rispecchiano gli intendimenti generali del Legislatore e possono essere anche un riferimento generale alla normativa per ogni attività che gestisce dati da tenere sotto controllo.
- la seconda è l'Applicazione del Codice ad un Rotary Club.
- la terza, è una bozza di “Documento Programmatico sulla Sicurezza” (DPS) che va personalizzato da ciascun Club recependo la propria organizzazione interna e le modalità della gestione dei dati relativi ai Soci. Il DPS, una volta compilato e stampato, deve essere vidimato con data certa entro il 31 Dicembre 2005 o comunque alla sua emissione.
- La quarta è costituita da una serie di bozze di lettere e dichiarazioni che consentono di attribuire le specifiche responsabilità ai soggetti interessati.
- Appendice: Guidelines for the use of electronic communications in Rotary International.



Parte Prima

1. Premessa

Chiunque ha diritto alla protezione dei dati personali che lo riguardano. Tutti i trattamenti di dati svolti all'interno di una attività (Club) sono e devono essere svolti esclusivamente per le finalità connesse alla realizzazione dell'oggetto sociale e pertanto il trattamento degli stessi è strumentale e strettamente correlato alle finalità del sodalizio: non è pertanto consentito alcun tipo di trattamento di dati che non sia in linea con gli scopi del Club.

Es.: Uso personale per invio messaggi promozionali, circolari aziendali, offerte, etc.

Gli strumenti, i sistemi, le applicazioni, gli archivi, le aree ed i luoghi di lavoro e quant'altro venga in concreto messo a disposizione per il trattamento, la custodia e la conservazione dei dati personali devono e dovranno essere utilizzati esclusivamente per le predette finalità di gestione delle attività del Club.

Tutti coloro che trattano dati personali e/o dati sensibili e/o giudiziari tramite strumenti informatici sono obbligati all'adozione delle Misure Minime di Sicurezza (MMS) ed in particolare tra queste a redigere il Documento Programmatico sulla Sicurezza (DPS) ed a riferire in fase di redazione di bilancio dell'avvenuta compilazione ed aggiornamento di detto documento.



2. Riferimenti

La materia è stata disciplinata, nel tempo, con le leggi:

- D. Lgs. 675/1996 “Protezione dei dati”
- D. Lgs. 166/1999 “Attuazione della Direttiva 96/9/CE relativa alla tutela giuridica delle banche dati”
- DPR 318/99 “Norme per l’individuazione delle misure minime di sicurezza per il trattamento dei dati personali”
- D. Lgs. 196/2003 “Codice in materia di protezione dei dati personali”

La finalità della normativa in materia è di regolamentare il trattamento, sia informatico che cartaceo, dei dati personali.

Il “Codice” (completo), è scaricabile dal sito Internet del Garante della Privacy

(www.garanteprivacy.it).



3. Finalità

Il testo unico, di seguito denominato "codice", garantisce 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.

Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione tramite qualsiasi canale (informatico e non).



4. Definizioni

Il testo unico, di seguito denominato "codice", garantisce 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.

Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione tramite qualsiasi canale (informatico e non).

4.1 Trattamento di dati personali

Per trattamento di dati si intende 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.

E' sufficiente anche una sola delle operazioni elencate per ritenere in corso un trattamento di dati personale.



4.2 Dato personale

Per dato personale si intende 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; si considera tale il dato oggettivo, ma anche il dato valutativo.

4.2.1 Dati identificativi

Per dati identificativi si intendono i dati personali che permettono l'identificazione diretta dell'interessato.

Possono essere: indirizzo abitazione, telefono e Società, indirizzo, telefono, fax, e-mail, cellulare, nome del coniuge.

4.2.2 Dati sensibili

Sono "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, organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

4.2.3 Dati giudiziari

Sono "dati giudiziari" i dati personali idonei a rivelare provvedimenti 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 del codice di procedura penale.



4.3 Banca dati

È "banca di dati" qualsiasi complesso organizzato di dati personali, (archivio) ripartito in una o più unità dislocate in uno o più siti.

4.4 Titolare del trattamento

"Titolare" del trattamento è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione ed organismo a cui competono, anche insieme ad altro titolare, le decisioni in ordine ai modi ed alle finalità del trattamento, alle modalità ed all'adozione delle misure di sicurezza.

Il titolare può designare un "responsabile" preposto al trattamento dei dati.

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi, altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza attraverso il suo Rappresentante pro-tempore.

In un Rotary Club, titolare del trattamento è il club, rappresentato dal Presidente pro-tempore.

4.5 Responsabili del trattamento

Il "responsabile" è la persona fisica, la persona giuridica od organismo preposti dal titolare al trattamento di dati personali; in sostanza è il soggetto cui sono affidate le incombenze di privacy (curare le informative, l'adeguamento alle misure di sicurezza, fornire direttive agli incaricati del trattamento, ecc.). Solo il titolare può nominare i responsabili del trattamento. Naturalmente il Responsabile del trattamento può avvalersi di collaboratori per lo svolgimento dei propri compiti.



La nomina del Responsabile è facoltativa, ma l'opportunità di nominare uno o più responsabili del trattamento cresce con l'aumento della articolazione organizzativa della propria struttura.

Si possono nominare più responsabili del trattamento, anche esterni al proprio ente, se ciò è reso necessario dall'esigenza della divisione dei compiti.

In un Rotary Club si può identificare quale Responsabile il Vice Presidente o il Segretario del Club fermo restando l'autonomia organizzativa di ciascun club.

4.5.1 Gli incaricati

Incaricato è la persona fisica che, pur non essendo stata nominata Responsabile, esegue le operazioni di trattamento su indicazione del titolare o del responsabile, osservando le loro prescrizioni.

Deve essere individuato per iscritto.

Le operazioni di trattamento possono essere effettuate solo da incaricati che, operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

La designazione degli incaricati è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

La formazione è obbligatoria nel caso in cui gli incaricati dal trattamento utilizzino con procedure elettroniche dati sensibili e/o giudiziari.

In un Rotary Club si possono identificare quali Incaricati il Segretario, il Tesoriere, il Prefetto e gli addetti alla segreteria (se esistono).



4.6 L'interessato

Interessato è la persona fisica, la persona giuridica, l'Ente o l'Associazione cui si riferiscono i dati personali; che gode dei diritti previsti dal codice della privacy.

Gli interessati hanno il diritto di ricevere l'informativa e di prestare il consenso per il caso della comunicazione all'esterno e della diffusione. Il Codice prevede una serie di diritti: di accesso ai dati personali, rettificazione dati inesatti, aggiornamento dati vecchi, integrazione dati incompleti, opposizione al trattamento, blocco e cancellazione dei dati trattati in maniera illegittima. Per esercitare i propri diritti l'interessato può ricorrere al Garante o al giudice ordinario in caso di inadempienze.

In particolare è possibile conoscere origine dei dati, finalità e modalità del trattamento, estremi del titolare e del responsabile e i soggetti ai quali possono essere comunicati i dati. E' possibile ottenere l'aggiornamento, la rettifica, l'integrazione dei dati o la cancellazione se trattati in violazione della normativa. La richiesta di esercizio dei diritti può essere inviata al titolare o al responsabile anche via fax o in posta elettronica e può essere rinnovata dopo 90 giorni. Il titolare ha 15 giorni per rispondere, che raddoppiano in casi di particolare complessità. Le modalità di risposta previste sono: estrazione di dati, comunicazione in forma intelligibile, consegna di copia di atti e documenti con i dati di terzi oscurati quando l'estrazione è difficile.

Se i dati non hanno natura "sensibile" (in quanto non attengono, ad esempio, alla sfera della salute, delle abitudini sessuali o delle convinzioni politiche, religiose e sindacali), la raccolta o l'elaborazione dei dati può essere basata sul consenso dell'interessato manifestato anche oralmente (purché documentabile per iscritto) oppure su un'ampia serie di presupposti equipollenti (es.: i dati siano estratti da un archivio pubblico accessibile a chiunque).

In un Rotary Club "Interessati" sono i soci che sottoscrivono il modulo di consenso. (vedi allegato 4)

Nel caso del Rotary, non vi è dubbio che gli interessati siano i Soci e, per certi versi ed entro certi limiti, i candidati Soci. Rotary Club nel suo complesso, in quanto associazione etc. gode dell'esenzione prevista dall'art. 24 (h) del Codice, che così recita: "Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento, **con esclusione della comunicazione all'esterno e della diffusione** è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati nell'atto di informativa ai sensi dell'art. 13"



4.7 Garante

E' l'Autorità di garanzia Nazionale in ordine all'attuazione delle norme sulla Privacy.

4.8 Comunicazione

Comunicazione significa dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

4.9 Diffusione

Diffusione significa dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

4.10 Informativa

L'informativa è il presupposto fondamentale per il consenso, in quanto mette in condizioni l'interessato di conoscere i propri diritti per poterli esercitare. L'informativa deve essere fornita prima dell'inizio della raccolta dei dati, può essere scritta o orale, deve essere chiara e corretta, resa con modalità semplificate. Deve segnalare le modalità di trattamento dei dati e indicare la natura obbligatoria o facoltativa del conferimento dei dati.

Le informazioni all'interessato presso il quale sono raccolti i dati possono essere fornite per scritto od oralmente; la forma scritta è richiesta obbligatoriamente se il trattamento riguarda dati sensibili, nel qual caso deve anche essere citata la disposizione che ne impone il trattamento.

L'interessato o la persona presso la quale sono raccolti i dati personali devo-



4.7 Garante

E' l'Autorità di garanzia Nazionale in ordine all'attuazione delle norme sulla Privacy.

4.8 Comunicazione

Comunicazione significa dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

4.9 Diffusione

Diffusione significa dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

4.10 Informativa

L'informativa è il presupposto fondamentale per il consenso, in quanto mette in condizioni l'interessato di conoscere i propri diritti per poterli esercitare. L'informativa deve essere fornita prima dell'inizio della raccolta dei dati, può essere scritta o orale, deve essere chiara e corretta, resa con modalità semplificate. Deve segnalare le modalità di trattamento dei dati e indicare la natura obbligatoria o facoltativa del conferimento dei dati.

Le informazioni all'interessato presso il quale sono raccolti i dati possono essere fornite per scritto od oralmente; la forma scritta è richiesta obbligatoriamente se il trattamento riguarda dati sensibili, nel qual caso deve anche essere citata la disposizione che ne impone il trattamento.

L'interessato o la persona presso la quale sono raccolti i dati personali devo-



no essere previamente informati oralmente o per iscritto circa:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato;
- gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti, è indicato tale responsabile.

L'informativa contiene anche gli elementi previsti da specifiche disposizioni del codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

La disposizione di cui sopra non si applica quando i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria, ecc. (vedi "Codice").

In un Rotary Club l'informativa è una dichiarazione che, per i nuovi soci, è riportata in calce al modulo di adesione al club (vedi allegato n. 2).

4.11 Consenso

Il trattamento di dati personali da parte di privati è ammesso solo con il consenso espresso dell'interessato.

Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.



5. Misure di sicurezza (all. B al “Codice”)

I dati personali oggetto di trattamento sono 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.

Le Misure Minime di Sicurezza (MMS) sono l'insieme degli accorgimenti tecnici ed organizzativi che bisogna adottare per assicurare almeno il livello minimo di sicurezza per la protezione dei dati personali; esse costituiscono tuttavia solo una parte degli accorgimenti obbligatori in materia di sicurezza. Si distinguono le misure minime di sicurezza (MMS) e le misure ulteriori di sicurezza: l'osservanza delle prime esclude responsabilità penali; l'osservanza delle seconde elimina responsabilità per risarcimento del danno.

In caso di trattamento con strumenti elettronici le MMS si possono sintetizzare in:

- Sistema di autenticazione informatica (user name, password).
- Sistema di autorizzazione (ove previsto).
- Adozione di firewall, antivirus.
- Redazione e aggiornamento periodico del DPS.

Vedi “Parte Terza”



6. Documento Programmatico per la sicurezza (DPS)

Si tratta di un documento "dinamico", destinato cioè ad essere periodicamente aggiornato, in particolare a fronte di cambiamenti significativi nella struttura dei dati trattati e delle relative misure di protezione; misure che in linea di principio sono determinate sulla base dell'Analisi dei Rischi.

La redazione del DPS è obbligatoria per tutti coloro, soggetti pubblici e privati, che

- si servono di strumenti elettronici
- siano il titolare di dati sensibili o giudiziari con qualunque tipo di trattamento. La categoria dei dati giudiziari è intesa in senso lato, e comprende anche altri dati personali, riferiti ad esempio a provvedimenti giudiziari non definitivi o alla semplice qualità di imputato o indagato.

Anche i soggetti che sono esonerati dall'obbligo di notifica del trattamento dei dati all'Autorità Garante, sono obbligati dalla normativa in oggetto alla stesura del DPS.

Si tratta di un manuale di pianificazione della sicurezza dei dati avente data certa, quale prova formale dell'adeguamento sostenuto.

In esso debbono essere descritti sia la situazione attuale (analisi dei rischi, distribuzione dei compiti e delle responsabilità, misure attuali di sicurezza dei dati) sia il percorso di adeguamento prescelto dalla struttura per adeguarsi alla normativa privacy.

Deve essere redatto entro il 31 Marzo 2006, ed adeguato entro il 31 marzo di ogni anno.

Ogni Rotary Club deve redigere ed adottare un DPS.



Parte Seconda

APPLICAZIONE del “CODICE” in un ROTARY CLUB

- **Titolare del trattamento** è il Club, rappresentato dal suo Presidente pro tempore.
- **Responsabile del trattamento** può essere il Vice Presidente o il Segretario
- **Incaricati del trattamento** sono Segretario, Tesoriere e Prefetto, gli addetti alla segreteria.
- Per evitare lettere annuali di nomina, si può precisare nel **Regolamento del Club**, una volta per tutte, quanto sopra.
- I dati personali comuni (nome, cognome, indirizzo, telefono abitazione) e non comuni (numero cellulare, indirizzo e-mail, nome del coniuge, società di appartenenza) devono essere comunicati al Club da parte dei Soci per le attività istituzionali di Club, Distretto e R.I. quali invio di bollettino, pubblicazioni, comunicazioni, corrispondenza, ecc.
- La **Informativa** corrispondente dovrà indicare:
 - le finalità e le modalità del trattamento cui sono destinati i dati;
 - la natura obbligatoria del conferimento dei dati;
 - le conseguenze di un eventuale rifiuto di aderire;
 - i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di distribuzione dei dati medesimi;
 - i diritti dell'interessato;
 - gli estremi identificativi del titolare del trattamento.

Sarà sufficiente specificare tutto ciò sulla **Scheda nuovo socio** di ammissione al Club.

La scheda va sottoscritta per accettazione dal Socio.

- La distribuzione dell'**Annuario** deve essere considerata “comunicazione”: pertanto lo stesso può essere fornito solo mediante controllo della distribuzione (registrazione dei riceventi).
- Per impedire la diffusione sia pure involontaria dei dati, tutti i messaggi/bollettini vanno inviati con gli indirizzi in Ccn (indirizzo occulto) .



- Misure Minime di Sicurezza (MMS) vanno applicate sia ai Data Base informatici che cartacei: per entrambi devono essere previste misure per impedirne il furto o la distruzione. Per gli archivi informatici in aggiunta si tratta di:
 - applicare password di accesso, antivirus e fire-wall ai PC che ospitano i suddetti data base
 - eseguire i regolari aggiornamenti dei programmi antivirus e fire wall; cambiare regolarmente la password
 - eseguire periodici back-up e salvataggi del data base
- Il Documento Programmatico sulla Sicurezza (**DPS**) va predisposto entro il 31/03/2006 e aggiornato annualmente entro il 31/03. Deve sostanzialmente indicare i nomi degli incaricati, la dislocazione fisica dei data base, confermare l'applicazione di password antivirus e fire-wall ai PC utilizzati. In esso debbono essere descritti sia la situazione attuale (analisi dei rischi, distribuzione dei compiti e delle responsabilità, misure attuali di sicurezza dei dati) sia il percorso di adeguamento prescelto dalla struttura per adeguarsi alla normativa privacy.

In allegato si riporta un fac-simile di DPS (Parte Terza)



IN CONCLUSIONE

Ogni Club deve:

- Definire per iscritto Responsabile e Incaricati del trattamento (per esempio una volta per tutte nel Regolamento) (allegato 3)
- Fornire a nuovi e vecchi soci la **Informativa** sull'utilizzo dei dati (allegato 2)
- Ottenere, sia da nuovi che da vecchi soci, il **Consenso** al trattamento dei dati personali (indispensabile per l'iscrizione al Club) e alla comunicazione all'interno dei Club dei propri dati, quale misura prudenziale ancorchè espressamente non richiesta dal codice, nonchè il consenso alla diffusione dei dati all'esterno del Club (allegato 2)
- Applicare le **Misure Minime di Sicurezza MMS** ai data base informatici e cartacei
- Predisporre il **Documento Programmatico sulla Sicurezza** e archivarlo con data certa (affrancatura e timbro postale)



Parte Terza

FAC-SIMILE

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DEI DATI DPS

1. Scopo

Il presente documento, denominato qui di seguito sinteticamente DPS, definisce e indirizza la politica per la sicurezza e la protezione dei dati personali. Esso descrive la struttura e l'organizzazione del sistema informatico e cartaceo operante, include una analisi dei rischi, dei trattamenti effettuati e delle misure in atto o da adottare per prevenire la loro distruzione, l'accesso abusivo e la dispersione. Per ogni tipo di rischio si indicano le conseguenze e l'elenco delle contromisure poste in essere come misura di protezione. Sono altresì indicate le modalità di accesso alla rete informatica, agli archivi cartacei e le responsabilità dei servizi coinvolti nel trattamento dei dati.

2. Riferimenti

- Decreto legislativo 30 giugno 2003, n. 196
- Legge 26 febbraio 2004, n. 45
- Disciplinare tecnico in materia di misure minime di sicurezza
- Sistema informatico (rete, server, PC, client, periferiche, utente, manutenzione, archiviazione, back-up, salvataggio)



3. Definizioni e abbreviazioni

- Titolare
- Responsabile
- Incaricati
- Amministratore di sistema
- Sistema informatico (rete, server, PC, client, periferiche, utente, manutenzione, archiviazione, back-up, salvataggio)

4. Dati personali

Ai fini del presente documento sono dati personali quelli individuati dall'art. 4.1 (b) del Codice.



5. Trattamento

I dati personali forniti dai soci sono utilizzati dal Club, dal Distretto e dal Rotary International esclusivamente per scopi istituzionali quali ad esempio fatturazioni, invio di documentazione, notiziari, riviste, ed ogni altro caso ritenuto istituzionale dai predetti Enti. Non è pertanto consentito al Club ed ai Soci alcun tipo di trattamento dei dati non autorizzato che non sia in linea con le finalità istituzionali del Club.

5.1 Titolare del trattamento

Titolare del trattamento è il Club, rappresentato dal Presidente pro-tempore sig.

5.2 Responsabile del trattamento

Responsabile del trattamento è il socio(o il vice Presidente/Segretario pro-tempore)

5.3 Incaricati del trattamento

Incaricati del trattamento sono i sig.ri,,(o il Segretario, il tesoriere, il prefetto pro-tempore, gli addetti di segreteria)



6. Elenco banche dati

In questo paragrafo vanno descritti le tipologie degli elenchi disponibili presso il Club e la loro localizzazione fisica:

- Elenco completo di indirizzi di tutti i Soci:
l'elenco è su supporto informatico ed è custodito presso.....
- Elenco completo dei pagamenti effettuati di tutti i Soci:
l'elenco è su supporto informatico ed è custodito presso.....
- Elenco completo delle attività professionali di tutti i Soci:
l'elenco è su supporto informatico ed è custodito presso
- Elenco completo dei componenti e famigliari di tutti i Soci:
l'elenco è su supporto informatico ed è custodito presso.....
-

7. Analisi dei rischi

I principali rischi sono:

- Accesso ai dati di personale o di terzi non autorizzati
- Eventi di forza maggiore tali da incidere su conservazione, accesso o reperibilità dei dati
- Comunicazione o diffusione non consentita
- Distruzione o perdita anche accidentale dei dati
- Manomissione, alterazione o danneggiamento degli strumenti, dei supporti, dei sistemi e delle applicazioni utilizzati per il trattamento dei dati
- Trattamento non consentito o non conforme alle finalità dell'associazione
- Appropriazione indebita di elenchi/archivi cartacei



8. Descrizione del sistema informatico

Il sistema informatico a disposizione del Club è indipendente/non indipendente da altro sistema operativo.

Esso opera attraverso l'aggiornamento dei dati inerenti l'attività del Club effettuati da uno/più addetti che ne hanno l'uso esclusivo/non esclusivo.

Ogni accesso al sistema è preceduto da autenticazione dell'operatore attraverso la richiesta di una pass-word che viene/non viene assegnata in forma controllata.

L'accesso alla rete Internet è preclusa/avviene attraverso un collegamento che richiede.....

Ogni anno, gli archivi elettronici vengono salvati su disco separato che viene archiviato e riposto.....(oppure) gli archivi vengono continuati garantendo la separazione gestionale.

Il back-up dei dati avviene in forma sistematica e regolare (possibilmente settimanale) attraverso la formazione di copia su dischetto/CD che viene archiviata

I programmi informatici che vengono utilizzati sono:

- ...
- ...
- ...

I programmi antivirus installati sono:

- ...
- ...

9. Misure fisiche di sicurezza

Le apparecchiature elettroniche e gli archivi cartacei sono protetti attraverso diversi sistemi che prevedono:

- Controllo degli accessi ai locali
E' controllato in quanto il sistema è alloggiato presso.....
- Sistemi di allarme e di sorveglianza
Sono presenti i seguenti apparati di allarme



- Custodia in classificatori o armadi non accessibili
Gli armadi contenenti la documentazione sono chiudibili con chiavi che sono custodite da.....
- Custodia dei supporti informatici rimovibili in contenitori ed armadi
Le caratteristiche dei contenitori contenenti i dischi di salvataggio dei dati informatici sono..... e l'accesso è riservato al personale di segreteria
- Dispositivi di sicurezza e antincendio
I locali nei quali sono custoditi gli archivi cartacei ed informatici sono dotati dei seguenti dispositivi antincendio: rilevatori di fumo, estintori.....
- Continuità dell'alimentazione elettrica
Le apparecchiature elettroniche sono/non sono dotate di gruppo di continuità che garantisce la presenza costante di energia elettrica
- Ecc.

10. Misure logiche di sicurezza

Le apparecchiature elettroniche e gli archivi cartacei sono protetti attraverso diversi sistemi che prevedono:

- Identificazione e autenticazione dell'utente (username e password) per l'accesso agli archivi informatici
- Controlli periodici per individuazione virus e aggiornamento periodico anti-virus
- Installazione e aggiornamento periodico firewall
- Aggiornamento periodico dei Sistemi Operativi
- Archiviazione, back-up e salvataggio dei dati
- Controllo e segnalazione di eventuali effrazioni per gli archivi cartacei

N.B.: Le password devono avere una lunghezza di almeno 8 caratteri



11. Misure organizzative di sicurezza

A seguito di quanto previsto dalla normativa, vengono di seguito individuate le seguenti figure incaricate di gestire e governare il sistema della gestione dei dati:

- Responsabile.....
- Incaricati.....
- Amministratore di sistema (se diverso dal Responsabile o da uno degli incaricati)

12. Formazione degli incaricati

Le persone coinvolte nella gestione dei dati hanno ricevuto adeguata informazione e formazione in merito ai contenuti dei requisiti legislativi

13. Controlli periodici

Il Responsabile del sistema provvede a regolari controlli periodici, almeno semestrali , che le procedure dichiarate siano rispettate e ne tiene traccia attraverso dichiarazioni sul bollettino del Club.

14. Aggiornamento del DPS

Il presente documento è soggetto ad aggiornamento periodico annuale, entro il 31/3, e le revisioni dovranno tenere conto anche dell'evoluzione legislativa nonché delle innovazioni della tecnica.



Parte Quarta

Allegato 1

MISURE MINIME DI SICUREZZA

E' indispensabile applicare le “Misure Minime di Sicurezza” (vedi DPR 318/99 “Norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali”, come dettagliato nel “Documento Programmatico sulla Sicurezza”.

La seguente lista rappresenta un pro-memoria di verifica i quanto applicato e quanto da introdurre al fine di rispettare quanto indicato nel DPS

Misure fisiche di sicurezza

- Controllo degli accessi ai locali
- Sistemi di allarme e di sorveglianza
- Custodia in classificatori o armadi non accessibili
- Custodia in armadi blindati ignifughi o cassaforte
- Custodia dei supporti informatici rimovibili in contenitori ed armadi
- Dispositivi di sicurezza e antincendio
- Continuità dell'alimentazione elettrica
- Ecc.

SI	NO



Misure logiche di sicurezza

- Identificazione e autenticazione dell'utente (username e password)
- Controlli periodici per individuazione virus e aggiornamento periodico anti-virus
- Installazione e aggiornamento periodico firewall
- Archiviazione, back-up e salvataggio dei dati

Misure organizzative di sicurezza

- Nomina di Responsabile, Incaricati, Amministratore di sistema
- Redazione di opportune linee guida e istruzioni interne (p. es. frequenza del back-up e salvataggio dati)



Allegato 2

FAC-SIMILE di dichiarazione da consegnare e ritirare per ogni Socio su carta intestata del Club.

Per i nuovi Soci sarà allegata alla lettera di adesione al Club

INFORMATIVA E CONSENSO (attività istituzionali)

Informativa e consenso ai sensi dell'art. 23 del d. Igs. n.196/03

Il Rotary Club è un'associazione non avente scopo di lucro, nata per realizzare progetti umanitari e di assistenza alle comunità, incoraggiare il rispetto di rigorosi principi etici in tutti i campi e soprattutto in ambito professionale, diffondere la pace e la buona volontà tra i popoli della terra.

Le precisiamo che i dati personali da lei fornitici verranno trattati nel pieno rispetto della disciplina sulla privacy e, in ogni caso, in conformità con quanto stabilito dal Garante per la Protezione dei Dati Personali con l'autorizzazione n. 3/2002 (e le successive autorizzazioni che verranno emanate in materia).

I dati da Lei conferiti saranno trasmessi anche al Distretto e al Rotary International per attività istituzionali strettamente connesse con gli scopi dell'associazione: essi verranno trattati con strumenti informatici e cartacei e serviranno alla nostra Associazione ai fini di iscrizione alla stessa e per permettere l'invio di documentazione, bollettini, riviste, ecc. I dati verranno in ogni caso trattati rispettando idonee misure di sicurezza in modo da impedire, o di ridurre al minimo, i rischi di distruzione o perdita dei dati, nonché di accesso non autorizzato o di trattamento non autorizzato o non consentito.

Il conferimento dei dati da parte Sua ha natura facoltativa ma qualora Lei decida di non fornirli, la Sua iscrizione non potrà essere accettata e ciò non consentirà la Sua partecipazione alle attività associative.

I dati da Lei conferitici non verranno diffusi né comunicati ad altri soggetti oltre quelli citati.

Il Titolare al trattamento dei Suoi dati personali è il Rotary Club, con sede in



Parte Quarta - Dichiarazione Informativa

Il Responsabile al Trattamento dei Suoi dati personali è

In ogni caso Lei avrà la facoltà di esercitare i diritti previsti dell'art. 23 del d. Lgs. n.196/03 e, in particolare, ha il diritto di conoscere i Suoi dati trattati dalla nostra associazione, di farli integrare, modificare o cancellare per violazione di legge, o di opporsi al loro trattamento per motivi legittimi; a tal fine, per esercitare tali diritti, può rivolgersi al Responsabile del Trattamento dati presso la sede su indicata.

Data

Firma:..... Presidente del Rotary Club

Data

socio del Rotary Club per presa visione ed informazione

Firma:.....



Allegato 3

FACSIMILE DI LETTERA DI INCARICO

Questo documento è un modello che contiene gli elementi essenziali di una Lettera di Incarico da redigere su carta intestata del Club.
Dovrà eventualmente essere adattato secondo le modalità concrete specifiche della attività di ogni Club

LETTERA DI INCARICO AI SENSI
DELL' ART. 30 DEL D. LGS. 30 GIUGNO 2003
N. 196 E ISTRUZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Con la presente La autorizziamo, nella qualità di Incaricato ex art. 30 del Decreto Legislativo 196/2003, al trattamento dei dati personali contenuti nelle banche dati ed archivi, automatizzati e non automatizzati, di cui il R. C. è titolare in quanto ciò sia necessario allo svolgimento delle attività da Lei prestate con il predetto club.

I dati personali al cui trattamento Lei è autorizzato sono dati personali comuni e non, relativi ai soci del club, di natura anagrafica e professionale trattati anche con l'ausilio di mezzi elettronici.

Trattasi di dati di contenuto riservato, che non possono essere divulgati e possono essere comunicati a terzi solo se ciò è richiesto dal Titolare o necessario per svolgere le attività di cui Ella sia incaricato nell'ambito dell'azione del Rotary International. Le ricordiamo che nel trattamento dei suddetti dati Lei è tenuto ad osservare, in quanto applicabili e per quanto di Sua competenza, le norme dettate dal D.Lgs. 196/2003 in materia di tutela dei dati personali, e in particolare l'art. 11 (modalità di trattamento dei dati), l'art. 13 (informazioni da rendere all'interessato), gli artt. 23 e 24 (consenso dell'interessato), l'art. 25 (divieti di comunicazione e diffusione dei dati), l'art. 31 (obblighi di sicurezza dei dati), gli artt. dal 33 al 36 e l'Allegato B (misure minime di sicurezza nel trattamento dei dati), nonché le istruzioni impartite dal Titolare con la presente.

Non è ammesso l'accesso di terzi al/ai personal computer/s da Lei utilizzato/i.



Nell'eventualità che i dati siano contenuti in memorie elettroniche, Lei è tenuto a proteggere l'accesso attraverso una password che Lei dovrà autodeterminare, che sarà nota a Lei solo, non dovrà contenere riferimenti a Lei agevolmente riconducibili e che Lei dovrà provvedere a modificare (almeno ogni tre/sei mesi se sono trattati dati sensibili) come prescritto dalla legge.

Lei è tenuto inoltre a custodire i dati su supporto cartaceo o altri supporti mobili che si trovino, anche provvisoriamente, nella Sua disponibilità, in modo da assicurare che non vi accedano soggetti non autorizzati e non possano essere danneggiati o distrutti.

Dettagliare eventuali regole per la custodia dei documenti, floppy disk, CD ecc.). Lei è tenuto a informare tempestivamente il Titolare (oppure, se nominato, anche il Responsabile) qualora abbia conoscenza del verificarsi di eventi che mettano a repentaglio la sicurezza dei dati quali per esempio: l'accesso agli strumenti elettronici utilizzati per il trattamento di soggetti non autorizzati; la violazione o mancata applicazione delle nostre regole fissate per a garantire la sicurezza dei dati personali; l'accesso a locali e archivi dove sono custoditi dati personali da parte di soggetti non autorizzati: qualsiasi caso di smarrimento, sottrazione, distruzione, trattamento illecito di dati;

Il Titolare del trattamento, in persona del Responsabile Sig..... {se nominato), è disponibile a fornirLe ogni ulteriore chiarimento che ritenesse necessario sull'applicazione della normativa di tutela dei dati personali.

La preghiamo di restituirci copia della presente controfirmata per ricevuta ed accettazione dell'incarico.

Cordiali saluti

.....2005

Il Titolare

(Presidente del Rotary Club)

Per ricevuta:

Il Responsabile del Trattamento.....

(Vice Presidente o Segretario del Rotary Club....)

..... 2005

L'incaricato del Trattamento:

(segretario, tesoriere, prefetto, addetti alla segreteria)

..... 2005



Allegato 4

FAC-SIMILE di dichiarazione da consegnare e ritirare per ogni Socio su carta intestata del Club.

Per i nuovi Soci sarà allegata alla lettera di adesione al Club

INFORMATIVA E CONSENSO PER DATI PERSONALI

Caro Socio,

Il Rotary Club predispone e distribuisce ai Soci e ad alcune organizzazioni esterne una elenco (es: rubrica) contenente i dati personali dei soci. Tali dati possono circolare all'interno del Club per le finalità istituzionali del sodalizio.

Poiché riteniamo utile fornire nel novero dei dati personali la foto dell'interessato, i riferimenti della società/ente presso il quale lavora, il numero di cellulare, l'indirizzo e-mail, il numero di fax, il nome del coniuge, con la presente si richiede il consenso dell'interessato alla diffusione di tali dati anche all'esterno del Club.

Detto consenso può essere fornito anche solo per alcuni dati e pertanto chiediamo di confermarci caso per caso i dati:

- Riferimenti della società/ente lavorativo sì / no
- Numero di cellulare sì / no
- Indirizzo e-mail sì / no
- Numero di fax sì / no
- Nome del coniuge sì / no
- Foto sì / no
-



In ogni caso avrai la facoltà di esercitare i diritti previsti dell'art. 23 del d. Lgs. n.196/03 e, in particolare, il diritto di conoscere i tuoi dati trattati dalla nostra associazione, di farli integrare, modificare o cancellare per violazione di legge, o di opposti al loro trattamento per motivi legittimi; a tal fine, per esercitare tali diritti, puoi rivolgerti al Responsabile del Trattamento dati presso il Club.

Il Presidente

Il socio per conferma dati

.....

data.....



APPENDICE

GUIDELINES

FOR THE USE OF

Electronic Communications

IN

ROTARY INTERNATIONAL

[Adopted by the Board of Directors of Rotary International in Decision #166, in November 2000]

*Electronic communication is fast becoming the preferred method of communication in our Rotary world. These **Guidelines** have been developed to promote the efficient and effective use of electronic communication.*

Use and Privacy of Email Addresses

Rotary Leaders and Rotarians interested in future Leadership positions at any level of Rotary are strongly encouraged to both have Email addresses and use the Internet. (See RI Board recommendation November 1999) When a Rotarian submits their Email address to the club, district or Rotary International, the Rotarian thereby acknowledges and agrees that Rotary may use the Email address for purposes of Rotary communication at that level. Rotarians who accept leadership positions acknowledge and accept that their Email addresses will be used for Rotary communication as appropriate at all levels of Rotary International.

No one should freely distribute Email addresses without the owner's consent. Similarly, forwarding of Email should not be done without first obtaining permission of the initiating author.



Group and Broadcast Email

No Rotarian should be added to an “e-groups” or other type of bulk mailing list without that person’s permission; excepting mailing lists specifically established for RI Directors, Trustees, and Officers (including, but not limited to District Governors, District Governors Elect, District Governors Nominee), as well as RI Committee members, RI Task Force Chairmen and Coordinators, DICOs, CICOs, and Club President. By virtue of having accepted the duties and responsibilities of their positions, Rotarians included in the “exception” list shall be presumed to have given permission to receive Email pertaining to their positions.

Whenever possible, one to one Emails are encouraged. When essential for efficiency,

Emailing to a select group of Rotarians directly involved in a particular task or interested in a particular subject is acceptable. Copying Rotarians who may not need to receive the Email is discouraged, to help minimize the of Email received. quantity

finito di stampare nel mese di dicembre 2005
Litowarr srl

Si ringrazia



ISTITUTO DI CERTIFICAZIONE DELLA QUALITÀ

ENGINEERING
& **SERVICE**

QUALITÀ E SICUREZZA



INQAS ITALIA

QUALITÀ, AMBIENTE E SICUREZZA

NORTON ROSE

Studio legale



QUALITÀ, AMBIENTE E SICUREZZA

