La PRIVACY

linee guida ad uso delle associazioni di volontariato

Il testo del presente fascicolo “La privacy Linee guida ad uso delle associazioni di volontariato” è a cura di Bruna Sartena e Nevio Meneguz operatori del CSV Belluno.
Gli autori ringraziano: “Luisa Vallese, Dottore Commercialista, esperto non profit e consulente dei CSV di Belluno, Rovigo e Verona, per la stesura della premessa; la sua competenza ha arricchito e completato il nostro lavoro tecnico; il dottor Alberto Pinto, i cui preziosi suggerimenti ci hanno sostenuto nel procedere con la precisione richiesta dal tipo di lavoro e l’Avv. Davide Cester, consulente legale del Csv di Padova, per le integrazioni e precisazioni a queste Linee Guida, nonché per il modello di Documento Programmatico sulla Sicurezza ad uso della associazioni che si allega”.

Il CSV di Verona ringrazia il CSV di Belluno per aver messo a disposizione gratuitamente il materiale.
Il fascicolo è presente sul sito internet www.csv.verona.it

LA PRIVACY
LINEE GUIDA AD USO DELLE ASSOCIAZIONI DI VOLONTARIATO

PREMESSA

Nell'attuale società, definita la "società della comunicazione", i dati personali hanno un valore determinante.
Si sente la necessità, soprattutto con lo sviluppo delle tecnologie, di proteggere la sfera privata dell'individuo e il suo diritto alla riservatezza. Tutelare la privacy quindi significa consentire all'individuo di difendere la propria sfera privata, scegliere il proprio stile di vita senza interferenze, decidere autonomamente l'ambito entro cui i suoi dati personali possono essere messi a conoscenza di terzi e di controllare i trattamenti di tali dati, nel rispetto delle esigenze della società in cui vive.
A tal proposito è entrata in vigore il 1° gennaio 2004 la nuova disciplina sulla privacy, contenuta nel Decreto Legislativo n. 196 del 30 giugno 2003, detto "Testo Unico" o "Codice in materia di protezione dei dati personali" (pubblicato sulla Gazzetta Ufficiale n. 174 del 29/07/2003 - suppl. ordinario n. 123). Essa ha lo scopo di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle liberta fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

LE PAROLE CHIAVE

Privacy è il diritto di costruire liberamente e difendere la propria sfera privata, di scegliere il proprio stile di vita senza interferenze ed intromissioni indesiderate da parte di terzi.
Tutelare la privacy significa consentire all'individuo di decidere autonomamente l'ambito entro cui i suoi dati personali, che ne rivelano l'identità e la sfera intima, possono essere portati a conoscenza di terzi e di controllare i trattamenti di tali dati, nel rispetto peraltro delle esigenze della società in cui vive.

Banca di dati è qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento (art. 4 comma 1 lettera p T.U.).

Dato personale è "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" (art. 4, comma 1, lett. b T.U.).

Dato identificativo è quel dato personale che permette l'identificazione diretta dell'interessato (art. 4 comma 1, lett. c T.U.).

Dato anonimo è quel dato personale che, in origine o a seguito di trattamento, non può essere associato a un soggetto identificato o identificabile.

Dato sensibile è esclusivamente il dato definito dall'art. 4 comma 1 lett. d) del Codice che rileva l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché idoneo a rivelare lo stato di salute e la vita sessuale.

Dato giudiziario è quel dato idoneo a rivelare provvedimenti di cui all'art. 3 comma 1 lett. da a) a o) e da r) a u) del DPR 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dai relativi carichi pendenti, o la qualità di imputato e da indagato, ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4 comma 1 lett. e T.U.).

Trattamento è "qualunque operazione o complesso di operazioni, effettuate 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." (art. 4. lett. a. T.U.)

Titolare è "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono le decisioni in ordine alle finalità e alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza" (art. 4. lett. f. T.U.).

Incaricati sono "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile" (art. 4. lett. h. T.U.). L'incaricato "opera sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite" (art. 30 T.U.).

Interessato è "la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali" (art. 4. lett. i. T.U.).

Responsabile del trattamento è "il soggetto preposto dal titolare al trattamento dei dati" che "per esperienza, capacità e affidabilità fornisce idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento, ivi compreso il profilo della sicurezza". Il responsabile si deve attenere alle istruzioni del titolare e i suoi compiti sono specificati per iscritto da quest'ultimo al momento della nomina (art. 4. lett. g, e art. 29 T.U.).

Comunicazione è "dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione" (art. 4 comma 1 lett. 1 T.U).

Diffusione è "dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"(art. 4 comma 1 lett. m T.U.).

ELENCO DEI FAC-SIMILE DI DOCUMENTO, DI SEGUITO RIPORTATI, PER RISPONDERE A STANDARD MINIMI DI SICUREZZA DEI DATI

Documento n. 1

DICHIARAZIONE DELL'ASSOCIAZIONE - NOMINA DEL RESPONSABILE DEL TRATTAMENTO E LINEE GUIDA DELL'ADEGUAMENTO APPLICAZIONE MISURE MINIME DI SICUREZZA

a) indicazione del "TITOLARE DEL TRATTAMENTO" e nomina del "RESPONSABILE".
Sono previsti i casi più frequenti di trattamento dei dati personali; l'Associazione individuerà e segnerà quelli coincidenti con le proprie caratteristiche.
Il documento dovrà essere firmato anche dal Responsabile del Trattamento – se nominato – per accettazione e per ricevuta del materiale; si precisa che la nomina del responsabile non è obbligatoria, anche se consigliata per "sgravare" il Presidente o i membri dell'organo direttivo di incombenze tecniche e organizzative relative soprattutto ai trattamenti informatici. Responsabile può essere nominato anche il Presidente, oppure un membro del Consiglio Direttivo, un aderente, il segretario, un dipendente se esiste. Tuttavia bisogna tenere presente che la nomina di un Responsabile del trattamento non elimina la responsabilità del Titolare (Odv) o della persona fisica che ha svolto un trattamento illecito o dannoso. Per questo il Presidente, anche se ha nominato un Responsabile, deve prestare attenzione agli adempimenti in tema di privacy e far sì che l'associazione se ne faccia carico, deve dare al responsabile apposite istruzioni e vigilare sul suo operato.

b) elenco dei criteri e delle procedure da adottare per garantire livelli minimi di sicurezza, sia per i dati conservati su supporti cartacei che per quelli conservati su supporti informatici.
Qualora l'Associazione tratti dati sensibili o giudiziari utilizzando supporti informatici sarà necessaria l'adozione del Documento Programmatico sulla Sicurezza (DPS) che completa l'intera documentazione sulla privacy riguardante le associazioni non profit. Si consiglia comunque la redazione del DPS a tutte le associazioni che svolgono un trattamento informatico di dati.

Documento n. 2

AUTORIZZAZIONE ALL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

Nomina dal responsabile di eventuali "INCARICATI del TRATTAMENTO". Questo documento è obbligatorio se il Responsabile utilizza altre persone che trattano i dati e, qualora si identifichino più persone "incaricate" a tale trattamento, il documento va sottoscritto da ognuna di esse per accettazione e per ricevuta della documentazione elencata.

Documento n. 3

ISTRUZIONI DEL TITOLARE SUL TRATTAMENTO DEI DATI

Il documento è suddiviso in due punti: punti 2a) e 2b). Essi saranno valutati sulla base delle modalità di archiviazione dei dati adottate dall'Associazione.

Documento n. 4

INFORMATIVE E RICHIESTE DI CONSENSO AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS. 196/2003

Questo documento è obbligatorio e va sottofirmato dall'interessato (socio, dipendente, collaboratore, ecc.); viene riportato per intero, ma l'Associazione potrà valutare i casi e potrà stendere il documento sulla base delle proprie caratteristiche.

Documento n. 5

SCHEDA DI ADESIONE ALLA ASSOCIAZIONE "....."

Fac-simile di scheda di adesione stilata nel rispetto della privacy, nella quale si chiede al socio l'autorizzazione ad utilizzare i suoi dati personali; essa va sottoposta all'aspirante nuovo socio e da questo sottoscritta. Sarà consegnata assieme al documento n. 4.

Documento n. 6

FORMULA PER L'ACQUISIZIONE DEL CONSENSO RELATIVO AL TRATTAMENTO DI DATI SENSIBILI

Fac simile di formula da adottare da parte di associazioni che trattano dati sensibili e/o giudiziari per l'acquisizione del consenso.

Documento n. 1

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

DICHIARAZIONE DELL'ASSOCIAZIONE - NOMINA DEL RESPONSABILE DEL TRATTAMENTO E LINEE GUIDA DELL'ADEGUAMENTO APPLICAZIONE MISURE MINIME DI SICUREZZA

Il/la sottoscritt..... nat... a.....
il..... e residente a..... in via.....
n..... CF..... rappresentante legale dell'Associazione
.....
dichiara di aver completato entro la data attuale il programma di adeguamento alle misure di sicurezza previste dal Decreto Legislativo 196/2003, articoli da 33 a 36 e allegato B.
Premesso che l'Associazione, TITOLARE del trattamento di dati personali, ai sensi del Decreto Legislativo 196/2003, art. 4, comma 1, lettera f), sulla tutela dei dati personali:

a) tratta (omettere le voci non considerate dall'Associazione):
   - dati comuni (generalmente il cognome e nome, il luogo e le data di nascita, la residenza);
   - dati sensibili (quelli da cui è possibile risalire alle opinioni politiche o religiose, oppure informazioni sulla salute, ecc.);
   - dati giudiziari (riguardano i dati contenuti nel casellario giudiziario, ad esempio: condanne penali e applicazione di misure di sicurezza)
   - dati comuni e sensibili;
b) utilizza (considerare solo le voci interessate):
   - archivi cartacei;
   - archivi cartacei e computer;
   - computer unico (uso interno);
   - più computer collegati in rete (uso interno);
   - Internet.

NOMINA

Il Signor..... nato a.....
il..... e residente a..... in via.....

n..... C.F. .....RESPONSABILE DEL TRATTAMENTO DEI *DATI (N.B. Non necessariamente il rappresentante legale dovrà essere nominato anche responsabile del trattamento. La nomina del responsabile non è obbligatoria anche se consigliata)*, ai sensi e per gli effetti dell'art. 29 del D.Lgs. 196/2003 con le precisazioni che seguono.

Sulla base di quanto premesso, vengono di seguito riportate le linee guida (i criteri e le procedure adottati e da adottare) per garantire il corretto trattamento e l'integrità dei dati:

- ricevuta l'informativa sull'utilizzazione dei dati personali, il socio autorizza il loro trattamento per il perseguimento degli scopi statutari;
- i dati del socio comunicati al responsabile o all'incaricato/i, vengono riportati su apposito registro e inseriti in computer;
- il registro dei soci è conservato in luogo sicuro e non accessibile al pubblico;
- eventuali documenti in originale o in copia, consegnati al responsabile o all'incaricato/i, sono conservati in archivi cartacei (contenitori/cartelline), tenuti sotto controllo dal responsabile o incaricato/i e posti in luogo non accessibile al pubblico;
- solo in caso di richiesta o interruzione del rapporto associativo, i documenti del socio vengono riconsegnati allo stesso o a un suo delegato;
- i dati vengono aggiornati su richiesta del socio o su necessità dell'Associazione;
- i dati vengono inseriti in computer dal responsabile o dall'incaricato/i, i quali sono muniti di password (che dovrà essere custodita da parte del responsabile o incaricato/i) e di codice identificativo personale;
- i floppy disk contenenti i dati dei soci devono essere custoditi in luogo non accessibile al pubblico, e in caso di riutilizzo, devono essere formattati per impedire la lettura dei dati precedenti;
- per l'utilizzo di Internet, l'elaboratore è dotato di un programma antivirus che dovrà essere aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno semestrale;
- hanno accesso ai dati conservati e trattati dall'Associazione, sia cartacei che inseriti in computer, le persone/incaricati del trattamento munite di apposita autorizzazione.

Le misure minime di sicurezza, di cui al previgente D.P.R. 318/99, vengono aggiornate con le disposizioni contenute negli articoli da 33 a 36 e nell'allegato B del D.Lgs. 196/2003 in modo che:

- le credenziali di autenticazione (password di accesso al p.c. e alla rete, nonché l'uso di una identificazione codificata per l'accesso ai software presenti) devono essere composti da almeno otto caratteri, modificati

almeno ogni sei mesi, con divieto assoluto di comunicazione del loro contenuto ad altri soggetti;
- in caso di prolungata assenza o impedimento dell'incaricato/i, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività del sistema, le credenziali di autenticazione di ogni incaricato, saranno utilizzate da parte di..... e custodite da parte di.....
- le credenziali di autenticazione devono essere disattivate nell'ipotesi di non utilizzo protratto per sei mesi, o di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
- i personal computer che contengono dati personali sono provvisti di software anti intrusione da parte di elementi esterni e di antivirus che già vengono aggiornati mensilmente;
- il salvataggio dei dati personali avviene da parte di un software di back up con scadenza almeno settimanale;
- ogni personal computer contenente dati personali deve essere spento quando non custodito direttamente dal titolare, anche se la mancata custodia sia per breve tempo.

Per una più puntuale osservanza degli obblighi di legge si rimanda al Documento Programmatico sulla Sicurezza (DPS), da adottarsi da parte di quelle associazioni che trattano dati sensibili e/o giudiziari per via informatica, e che comunque si consiglia a tutte le associazioni che svolgono un trattamento informatico di dati.

Luogo, data Firma del responsabile

Documento n. 2

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

AUTORIZZAZIONE ALL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

Il/la sottoscritt..... nat... a.....
il..... e residente in.....
CF..... rappresentante legale dell'Associazione
.....

PREMESSO CHE

l'Associazione di cui sopra è TITOLARE del trattamento dei dati personali, ai sensi dell'art. 4 lett. f e art. 28 del Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, in data....

DICHIARA

che la predetta Associazione ha nominato INCARICATO del trattamento dei dati personali il signor .....
nato a ..... il ..... e residente a.....
in via..... CF.....

COMUNICA QUANTO SEGUE:

1. L'incaricato è autorizzato al trattamento dei dati personali secondo le direttive impartite con il documento "Istruzioni del titolare sul trattamento dei dati" (*successivo documento n. 3 già consegnato all'INCARICATO del trattamento e da questo sottoscritto*);
2. quando sarà necessario verranno consegnati dal responsabile aggiornamenti ad integrazione del documento di cui al punto 1 del presente comunicato;
3. l'incaricato attesta di aver ricevuto materiale informativo inerente la tutela del trattamento dei dati personali;
4. l'incaricato attesta che il trattamento dei dati avviene per le finalità

esclusivamente indicate nella richiesta di adesione da parte del socio;
5. l'incaricato attesta di essere stato informato relativamente agli obblighi in materia di trattamento dei dati personali, sottoscrivendo la presente comunicazione.

Nello svolgimento dell'incarico, l'incaricato dovrà adottare tutte le misure necessarie, immediate e urgenti, al fine di procedere alla tutela dei dati, e segnalerà al Responsabile del trattamento dei dati l'opportunità di adottare ulteriori misure di sicurezza.
Nello svolgimento del compito, egli segnalerà al Responsabile e/o al Titolare eventuali reclami di soci, qualunque fatto che a suo avviso possa compromettere la sicurezza dei dati ed eventuali comportamenti da lui assunti in contrasto con le indicazioni fornite.

Copia della presente viene consegnata all'incaricato.

Data e luogo

Firma Il responsabile del trattamento .....
Firma L'incaricato del trattamento .....

Documento n. 3

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

ISTRUZIONI DEL TITOLARE SUL TRATTAMENTO DEI DATI

Il presente documento intende fornire una prima valutazione dei criteri tecnici ed organizzativi che sono stati adottati dall'Associazione al fine di ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati COMUNI e/o SENSIBILI, di accesso non consentito, non autorizzato o di trattamento non conforme alle finalità della raccolta.

1. PROTEZIONE DELLE AREE E DEI LOCALI

Contro i rischi di intrusione, l'ufficio è dotato di una porta munita di chiave di cui il Responsabile è in possesso.
elencare le altre persone a cui è stata consegnata la chiave (incaricato/i, altri…).
Si raccomanda di chiudere correttamente tutti gli accessi del locale contenente dati in supporto cartaceo (archivio e mobili contenenti documentazione con dati comuni e sensibili) e di collocare i mobili in luogo non accessibile al pubblico.
L'area del locale contenente i dati in supporto cartaceo è ubicata in modo tale che il responsabile e l'incaricato/i del trattamento possono rilevare a vista l'accesso non autorizzato da parte di persone estranee e di conseguenza impedirne l'accesso.

2. CRITERI E PROCEDURE PER ASSICURARE L'INTEGRITÀ DEI DATI

Di seguito si illustrano le misure adottate per garantire la sicurezza e l'integrità dei dati per:

a) Computer e supporti informatici.
In primo luogo si osserva che il computer risulta sollevato da terra in modo da evitare eventuali perdite di dati dovute ad allagamenti; in secondo luogo, si evidenzia che sono installati dispositivi che impediscono il danneggiamento dei dati in caso di sbalzi di tensione o di interruzione di corrente elettrica.

L'integrità dei dati è inoltre garantita mediante idonea procedura di salvataggio periodico (back-up) su floppy disk. Detti supporti di salvataggio vengono conservati e archiviati a cura del responsabile e/o dell'incaricato/i in un mobile munito di chiave e non accessibile a persone non autorizzate.
I floppy disk contenenti dati personali di soci, se non più utilizzati, devono essere formattati prima di essere riutilizzati da altre persone non autorizzate al trattamento, per impedire la lettura dei dati.
L'introduzione di password all'accensione del personal computer e dei relativi codici identificativi (nel caso di più persone autorizzate), ha determinato un livello di sicurezza circa i dati contenuti nei personal computer ritenuto soddisfacente.
Per quanto riguarda l'obbligo precedentemente previsto dall'art. 4 del DPR 318/99 (ora abrogato) e dal n. 16 del vigente Disciplinare Tecnico allegato sub B al D.Lgs. 196/03, l'elaboratore è dotato di programma antivirus che viene aggiornato sotto la responsabilità del titolare del trattamento (*o a cura del responsabile*) a cadenza almeno semestrale.
Nel caso in cui vengano trattati dati sensibili o giudiziari elettronicamente o in via informatica, si seguiranno anche le misure minime di sicurezza richieste dal Disciplinare Tecnico allegato al D.Lgs. n. 196/03 (nn. da 20 a 24) e descritte nel DPS allegato e redatto ai sensi dell'art. 34 e dell'allegato B (n. 19) del D.Lgs. n. 196/2003.

b) Supporti cartacei.
Criteri di protezione dei supporti cartacei.
Relativamente ai supporti cartacei, i criteri di protezione riguardano qualsiasi informazione e/o documento che viene consegnato all'Associazione.
I documenti vengono inseriti in cartelline e vengono conservati e archiviati a cura del responsabile e dell'incaricato/i in un mobile munito di chiave e non accessibile a persone non autorizzate.
Si ribadisce che il presente documento scaturisce da una prima analisi dei rischi e che si dovrà provvedere al suo aggiornamento nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro. L'incaricato del trattamento è obbligato ad uniformarsi a quanto contenuto nel presente documento ed il responsabile del trattamento è obbligato a vigilare sull'osservanza delle disposizioni da parte dell'incaricato.

Luogo e data

Firma Il responsabile del trattamento .....
Firma L'incaricato del trattamento .....

Documento n. 4

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

INFORMATIVA ALL'INTERESSATO (SOCIO, DIPENDENTE, COLLABORATORE, ECC.) E RICHIESTA DI CONSENSO AL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL DECRETO LEGISLATIVO 196/2003

Desideriamo informarla che, ai sensi dell'art. 13 del Decreto Legislativo n. 196/2003, i suoi dati personali, comunicatici all'inizio del rapporto con l'Associazione, saranno utilizzati per una o più delle seguenti finalità (indicare solo le voci interessate):

1. Trattamento dei dati sensibili, nell'ambito delle attività istituzionali e complementari dell'Associazione, svolto nelle modalità più idonee al raggiungimento con positività del risultato del servizio richiesto;
2. Trattamento dei dati comuni per tenuta della contabilità dell'Associazione, registro infortuni e tutti gli altri registri e documenti necessari alla amministrazione;
3. Compilazione della dichiarazione dei redditi e obblighi fiscali gravanti sull'Associazione;
4. Pagamento dei contributi previdenziali sia dell'INPS che di altri enti previdenziali, assicurativi INAIL, fiscali inerenti le ritenute d'acconto operate sulle competenze professionali o altro;
5. Compilazione, se richiesta, di modelli relativi alla richiesta di posizioni assicurative INPS, INAIL o altri enti assicurativi e previdenziali;
6. Compilazione, se necessaria, delle deleghe di pagamento "F24" relative alla gestione contabile-fiscale dell'Associazione, contributi dei soggetti sottoposti a contribuzione della gestione separata dell'INPS o di Casse di Previdenza istituite dalle Categorie Professionali, ivi compresa la comunicazione all'INPS o a dette Casse di Previdenza delle modalità di calcolo e/o versamento, pratiche INPS e Casse Previdenza in genere;
7. Invio e ricezione di circolari da parte di Enti alla nostra Associazione, per rispondere agli obblighi di legge.

Tali dati vengono trattati manualmente o a mezzo del sistema informatico,

sul quale vengono conservati e sul quale sono inoltre conservati i registri e tutto quanto serva all'amministrazione della nostra Associazione, comprese le dichiarazioni anche relative ad anni precedenti. Tali dati saranno cancellati da tale sistema nel momento in cui si sia prescritto per legge il termine per il controllo e l'accertamento degli adempimenti di cui sopra. I documenti tutti, registri, autorizzazioni, ecc. sono conservati anche nel nostro archivio informatico con l'utilizzo del sistema di archiviazione elettronica dei dati e saranno conservati per la durata richiesta dalla legge.
Precisiamo che, anche in assenza di detta richiesta, i Suoi dati potranno essere comunicati a seguito di ispezioni o verifiche all'Amministrazione Finanziaria ed agli Enti previdenziali, Agenzia delle Entrate, Ispettorato del Lavoro ed in genere a tutti gli organi preposti a verifiche e controlli circa la regolarità degli adempimenti di cui alle finalità anzi indicate.

EVIDENZIAMO CHE

il trattamento dei dati per le finalità sopra indicate è essenziale ai fini del regolare adempimento della gestione dell'Associazione
L'Associazione ha predisposto e perfezionerà ulteriormente il sistema di sicurezza di accesso e conservazione dei dati.

Titolare del trattamento dei dati è l'Associazione scrivente, con sede in ..... fax..... tel.....

Il Responsabile del trattamento è.....
(*N.B. Non necessariamente il rappresentante legale dovrà essere nominato anche responsabile del trattamento. La nomina del responsabile non è obbligatoria anche se consigliata*).

Incaricato è:
..... operante nell'ufficio della sede legale dell'Associazione..... Via .....
..... operante nell'ufficio della sede legale dell'Associazione..... Via .....
..... operante nell'ufficio della sede legale dell'Associazione..... Via .....

I dati verranno comunicati a .....

La informiamo inoltre che, compatibilmente alla responsabilità che grava su questa Associazione per l'assolvimento del servizio richiesto, l'art. 7 del Decreto Legislativo 196/2003, le conferisce i seguenti specifici diritti:

Art. 7 (Diritto di accesso ai dati personali e altri diritti).

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intellegibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di richiedere e di ottenere:
   a) l'aggiornamento, la rettifica e qualora lo ritenga necessario, l'integrazione dei suoi dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Per ciascuna richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) può essere chiesto all'interessato, ove non risulti confermata l'esistenza di dati che lo riguardano, un contributo spese, non superiore ai costi effettivamente sopportati, secondo le modalità di cui all'articolo 10 commi 7, 8 e 9 del Decreto Legislativo 196/2003.
Tutti i diritti suddetti relativi ai dati personali concernenti persone decedute possono essere esercitati da chiunque vi abbia interesse.

Nell'esercizio dei diritti suddetti, l'interessato può conferire, per iscritto, delega o procura a persone fisiche/associazioni.

Ai sensi dell'art. 13 D.Lgs. n. 196/2003 si ribadisce che il conferimento dei dati è necessario per il raggiungimento delle finalità dell'Associazione, per la gestione del rapporto associativo, per l'esecuzione e l'organizzazione del servizio e per l'adempimento degli obblighi di legge, tra cui quelli assicurativi, contabili e per riscossione di eventuali contributi.

Il conferimento dei dati relativi a ..... (es. numero di cellulare, impiego, titolo di studio .....) è facoltativo.

CHIEDIAMO

ai sensi dell'art. 23 D. Lgs. n. 196/2003, di manifestare per iscritto il Suo consenso al trattamento di detti dati.

Il/la sottoscritt..... nat... a.....
il..... e residente a.....
via..... C.A.P..... prov.....
Con la firma apposta alla presente attesta il proprio libero consenso affinché il/la titolare e il/la responsabile e/o l'incaricato/a procedano al trattamento dei Suoi dati personali e alla loro comunicazione nell'ambito dei soggetti indicati nell'informativa di cui sopra e per le finalità in essa indicate.

Data e luogo

Nome Cognome..... Firma.....

Documento n. 5

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

SCHEDA DI ADESIONE ALLA ASSOCIAZIONE "....."

Il/la sottoscritt..... nat... a.....
il..... residente a.....
via..... tel. ..... C.F. .....
chiede di divenire socio dell'Associazione "....."
e versa la quota di iscrizione di euro..... e dichiara di accettare quanto previsto dallo Statuto e dal Regolamento della Associazione.

Ricevuta l'informativa ai sensi dell'art. 13 del Decreto Legislativo 196/2003, consento al trattamento dei miei dati personali nella misura necessaria al perseguimento degli scopi statutari, e con le modalità indicate nell'informativa medesima.

Data e luogo

Nome Cognome..... Firma.....

n. libro soci..... n. tessera.....

Documento n. 6

Associazione .....

via ..... n. ..... loc. ..... prov. .....

C.F. .....

FORMULA PER L'ACQUISIZIONE DEL CONSENSO RELATIVO AL TRATTAMENTO DI DATI SENSIBILI

Il/la sottoscritt..... nat... a.....
il..... residente a.....
via..... n. .....
ricevute le informazioni di cui agli artt. 7 e 13 del Decreto Legislativo n. 196/2003 sulla privacy, acconsente al trattamento dei propri dati personali per il perseguimento degli scopi determinati, individuati e legittimi individuati dall'atto costitutivo e dallo statuto dell'Associazione, dichiarando di aver avuto conoscenza che i dati medesimi rientrano nel novero di quelli sensibili e/o giudiziari di cui all'art. 4, comma 1 lettere d) ed e) del D.Lgs. medesimo.

Data

Nome Cognome..... Firma.....

RIEPILOGO DEI PRINCIPALI ADEMPIMENTI

Sinteticamente:

A) Dati comuni
Informativa scritta o orale che indichi:
- finalità del trattamento;
- modalità del trattamento;
- titolare del trattamento;
- responsabile del trattamento, se nominato;
- facoltà per l'interessato di esercitare i diritti di cui all'art. 7 del Decreto Legislativo 196/2003;
- consenso, anche non scritto, da parte dell'interessato, previamente informato. ATTENZIONE: l'art. 23 richiede che il consenso sia "documentato per iscritto" ad opera del titolare/incaricato.

Per il trattamento di questi dati non è necessaria l'autorizzazione del Garante.

B) Dati sensibili (non idonei a rilevare lo stato di salute o la vita sessuale).
Informativa scritta o orale che indichi:
- finalità del trattamento;
- modalità del trattamento;
- natura dei dati sensibili;
- titolare del trattamento;
- responsabile del trattamento, se nominato;
- facoltà per l'interessato di esercitare i diritti di cui all'art. 7 del Decreto Legislativo 196/2003.

Per il trattamento dei dati sensibili, la norma generale (art. 26, comma 1, del Decreto Legislativo 196/2003) prevede la presenza sia del consenso che dell'autorizzazione.
Tuttavia l'art. 26, comma 4, deroga alla norma generale prevedendo la sola autorizzazione del Garante "quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto del-

l'informativa ai sensi dell'articolo 13". Il provvedimento ha in tal caso liberalizzato il trattamento dei dati sensibili dalla necessità di acquisire il consenso dell'interessato.
Questa esclusione riguarda però solo le associazioni *a carattere politico, filosofico, religioso o sindacale*. Si deve quindi ritenere che le Odvle quali, invece, nello statuto si richiamano genericamente a doveri e principi di solidarietà e altruismo (la maggior parte) *devono chiedere il consenso scritto* per il trattamento dei *dati sensibili* degli aderenti e di coloro che hanno con l'associazione contatti regolari.
Il Garante ha emesso, ai sensi dell'art. 40 del T.U., "Autorizzazioni tipo", che coprono buona parte dei trattamenti dei dati svolti dalle associazioni, ed in particolare:
- AUTORIZZAZIONE n. 3 del 30.6.2004 per il trattamento dei dati sensibili da parte degli organismi di tipo associativo e alle fondazioni, tra cui sono espressamente comprese le organizzazioni di volontariato e le ONLUS;
- AUTORIZZAZIONE n. 2 del 30.6.2004 per il trattamento dei dati idonei a rivelare lo stato di salute e al vita sessuale.

Il D. Lgs. n. 196/03 prevede anche un obbligo di notifica (comunicazione) al Garante dell'esistenza del trattamento. Tuttavia l'art. 37, comma 1, lett. c specifica che vanno notificati al Garante solo i trattamenti dei dati sulla vita sessuale o sulla sfera psichica trattati da associazioni, enti od organismi non profit che hanno carattere politico, sindacale, religioso o filosofico, tra cui non rientrano, ad esempio (parere del Garante 23.4.2004) le cooperative che svolgono attività di ricovero e assistenza a malati psichici.
I dati idonei a rilevare lo stato di salute non possono essere diffusi.

C) Dati giudiziari (i dati personali idonei a rilevare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u) del DPR 313/2002, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato).

Informativa scritta o orale che indichi:
- finalità del trattamento;
- modalità del trattamento;
- natura dei dati sensibili;
- titolare del trattamento;
- responsabile del trattamento;
- facoltà per l'interessato di esercitare i diritti di cui all'art. 7 del Decreto Legislativo 196/2003;

È necessaria inoltre l'autorizzazione del Garante.
Il Garante ha emesso una "Autorizzazione tipo" per il trattamento dei dati giudiziari da parte degli enti non profit (Autorizzazione n. 7 del 30.6.2004)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.)

Il DPS si presenta come la novità del Testo Unico e costituisce una sorta di manuale della sicurezza ai fini del trattamento dei dati personali tutelati dal Codice sulla privacy.
Questo documento rappresenta una opportunità per analizzare la situazione associativa ed organizzare le procedure a garanzia della sicurezza nei trattamenti.
Esso andrebbe redatto tuttavia, anche se in modo semplificato, ogniqualvolta l'associazione svolga un trattamento informatico dei dati, anche non trattandosi di dati sensibili e/o giudiziari.
Si tratta di un compito importante considerato che, quando è obbligatorio, la mancata predisposizione del DPS è sanzionata.
Il DPS non deve essere comunicato ad alcuno ma solo conservato presso la sede dell'associazione e deve avere data certa.
Per la redazione del DPS si può utilizzare l'apposito modello previsto dal Garante, seguendo le istruzioni e adeguandolo alla propria realtà associativa.

Il Documento Programmatico della Sicurezza viene di seguito riportato nella versione ad uso delle associazioni di volontariato *(redatta dall'Avv. Davide Cester)* ***integralmente, sia nella versione generica fornita dal Garante.***

GUIDA OPERATIVA PER IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (versione ad uso delle associazioni)

Documento programmatico sulla sicurezza nel trattamento dei dati personali[1]

Il presente documento è redatto ai sensi dell'art. 34, comma 1, lett. g) del D.Lgs. n. 196/03 (Codice della privacy) e al Disciplinare Tecnico allegato sub B (in seguito D.T.), con lo scopo di descrivere il quadro delle misure minime di sicurezza, organizzative, fisiche e informatiche, adottate dall'**Associazione di Volontariato** "....", con sede in....., via..... n. ....., *iscritta al Registro del Volontariato al n. ....*, al fine della tutela dei dati personali trattati dall'associazione medesima.
L'associazione svolge l'attività di.....[2].

Il presente DPS è redatto e firmato dal Presidente e legale rappresentante dell'Associazione, in seguito indicata anche solo come Titolare.
[oppure]
Il presente DPS è redatto e firmato dal Responsabile del trattamento signor.....[3], ...[4], nominato con lettera del.....

L'associazione svolge i seguenti trattamenti di dati personali nelle strutture indicate:

Codice del trattamento	Descrizione del trattamento	Natura dei dati	Struttura dove è svolto il trattamento	Responsabile della struttura
COD1				
COD2				
COD3				
COD4				
COD5				
.....				
.....				

I trattamenti possono comprendere il complesso di operazioni indicate nell'art. 4, comma 1, lett. a) ed in particolare 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 cancellazione e la distruzione dei dati, nei limiti e con le modalità descritte nel presente DPS e nell'informativa rilasciata all'interessato. La comunicazione dei dati avviene nei limiti di legge con riferimento a ciascun tipo di dato.

Codice del trattamento	Computer dove sono contenuti e trattati i dati	Dispositivi da accesso e tipologia di interconnessione	Localizzazione dei supporti di memorizzazione
COD1			
COD2			
COD3			
COD4			
COD5			
.....			
.....			

Codice del trattamento	Rischi derivanti dalle persone	Rischi derivanti dagli strumenti	Rischi derivanti dal contesto ambientale	Quantificazione del rischio
COD1				Alto/medio/basso
COD2				Alto/medio/basso
COD3				Alto/medio/basso
.....				

Misure di sicurezza per il trattamento con strumenti elettronici (p. 19.4. D.T.)

Rischio che si vuole contrastare	Misura adottata	Misura da adottare	Trattamento o banca dati interessata	Soggetto incaricato dell'adozione della misura e dei controlli	Periodicità e modalità dei controlli

Sarà inoltre adottata ogni altra misura che venisse ritenuta utile e necessaria dai tecnici, compatibilmente alle risorse dell'associazione, per migliorare la sicurezza degli strumenti elettronici.

Misure di sicurezza per i trattamenti non elettronici (p. 27-29 D.T.)

Rischio che si vuole contrastare	Misura adottata	Misura da adottare	Soggetto incaricato dell'adozione della misura e dei controlli	Periodicità e modalità dei controlli

Misure per il ripristino dei dati (p. 19.5. D.T.)

Computer o archivio informatico	Dati sensibili e/o giudiziari inseriti	Procedure di salvataggio	Soggetto incaricato del salvataggio e del ripristino	Localizzazione delle copie di sicurezza

Formazione degli incaricati (p. 19.6. D.T.)

Modalità della formazione	Categorie di incaricati interessate	Calendario	Relatore e responsabile della formazione
Corso presso la sede			

Trattamento da parte di soggetti esterni (p. 19.7. D.T.)

Trattamento svolto all'esterno	Soggetto che lo svolge	Impegni assunti in relazione alle misure di sicurezza

Il presente DPS è conservato presso la sede dell'associazione per essere esibito in caso di controllo; è a disposizione di ogni incaricato e verrà aggiornato entro il .....[6]

....., lì

Il legale rappresentante | Il responsabile

..... | .....

[1] *Questa versione di DPS è stata redatta sulla base delle indicazioni del Garante, che ha consentito l'inserimento di schemi e riquadri come quelli qui inseriti. Naturalmente i Titolari possono utilizzare le modalità che preferiscono nella redazione del DPS, che deve comunque contenere tutte le informazioni richieste dal Codice e dal Disciplinare Tecnico.*

[2] *L'indicazione dell'attività sociale è facoltativa.*

[3] *Nome e cognome.*

[4] *Qualifica all'interno dell'associazione (es. Presidente, dipendente, volontario…..)*

[5] *L'assistenza di una ditta esterna non è obbligatoria ma è una scelta dell'associazione. Qualora però ci si avvalga di una ditta esterna il D.T. al p. 25 stabilisce che questa rilasci il certificato di conformità (cioè "una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare Tecnico").*

[6] *L'aggiornamento del DPS deve essere per lo meno annuale, quindi si potrà scrivere, ad es. 8 aprile 2006 se il DPS è stato redatto l'8 aprile 2005.*

GUIDA OPERATIVA PER REDIGERE IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS) (versione Garante Privacy)

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

PREMESSA

La presente guida mira a facilitare l'adempimento dell'obbligo di redazione del documento programmatico sulla sicurezza (DPS) nelle organizzazioni di piccole e medie dimensioni o, comunque, non dotate al proprio interno di competenze specifiche[1].
La guida può essere di ausilio nella redazione del DPS, ma non è obbligatorio utilizzarla per adempiere all'obbligo.
La guida è strutturata in due parti: la prima contiene istruzioni per sviluppare il DPS negli aspetti descrittivi oppure nella compilazione di alcune tabelle riportate nella seconda parte.
Nella guida sono anche evidenziati altri elementi utilizzabili facoltativamente – comprese alcune tabelle –, che si ritengono utili per una più approfondita definizione del DPS.

PARTE I - ISTRUZIONI

Per ciascuna regola dell'Allegato B al Codice sono riportati i contenuti, le informazioni essenziali e gli ulteriori elementi da inserire nel DPS.

Elenco dei trattamenti di dati personali (regola 19.1)

Contenuti
In questa sezione sono individuati i trattamenti effettuati dal titolare, di-

[1] Nelle strutture di piccole dimensioni dove possono mancare specifiche competenze, si può anche chiedere consultare per alcuni profili tecnici il fornitore/installatore degli strumenti elettronici e del relativo software.

rettamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.
Nella redazione della lista si può tener conto anche delle informazioni contenute nelle notificazioni eventualmente inviate al Garante anche in passato.

Informazioni essenziali (v. anche tab. 1.1)
Per ciascun trattamento vanno indicate le seguenti informazioni secondo il livello di sintesi determinato dal titolare:
Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es., fornitura di beni o servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti o utenti, dipendenti e/o collaboratori, fornitori, ecc.).
Natura dei dati trattati: indicare se, tra i dati personali, sono presenti dati sensibili o giudiziari.
Struttura di riferimento: indicare la struttura (ufficio, funzione, ecc.) all'interno della quale viene effettuato il trattamento. In caso di strutture complesse, è possibile indicare la macro-struttura (direzione, dipartimento o servizio del personale), oppure gli uffici specifici all'interno della stessa (ufficio contratti, sviluppo risorse, controversie sindacali, amministrazione-contabilità.)
Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
Descrizione degli strumenti elettronici utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi).

Ulteriori elementi per descrivere gli strumenti (v. anche tab. 1.2)*
Identificativo del trattamento: alla descrizione del trattamento, se ritenuto utile, può essere associato un codice, facoltativo, per favorire un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle.
Banca dati: indicare eventualmente la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i da-

* Da indicare facoltativamente.

ti. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. In tal caso le banche dati potranno essere elencate.
Luogo di custodia dei supporti di memorizzazione: indicare il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano (in quale sede, centrale o periferica, o presso quale fornitore di servizi, ecc.) gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (nastri, CD, ecc.) ed ogni altro supporto rimovibile. Il punto può essere approfondito meglio in occasione di aggiornamenti.
Tipologia di dispositivi di accesso: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.
Tipologia di interconnessione: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.
Le predette informazioni possono essere completate o sostituite da schemi, tabelle, disegni di architettura del sistema informativo o da altri documenti aziendali già compilati e idonei a fornire in altro modo le informazioni medesime.

Distribuzione dei compiti e delle responsabilità (regola 19.2)

Contenuti
In questa sezione occorre descrivere sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati. Si possono utilizzare anche mediante specifici riferimenti documenti già predisposti (provvedimenti, ordini di servizio, regolamenti interni, circolari), indicando le precise modalità per reperirli.

Informazioni essenziali (v. anche tab. 2)
Struttura: riportare le indicazioni delle strutture già menzionate nella precedente sezione.
Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.
Compiti e responsabilità della struttura: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.). Anche in questo caso è possibile utilizzare, nei termini predetti, altri documenti già predisposti.

Analisi dei rischi che incombono sui dati (regola 19.3)

Contenuti
Descrivere in questa sezione i principali eventi potenzialmente dannosi per la sicurezza dei dati, e valutarne le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati.

Informazioni essenziali (v. anche tab. 3)
Elenco degli eventi: individuare ed elencare gli eventi che possono generare danni e che comportano, quindi, rischi per la sicurezza dei dati personali. In particolare, si può prendere in considerazione la lista esemplificativa dei seguenti eventi:

1) comportamenti degli operatori:
   - sottrazione di credenziali di autenticazione
   - carenza di consapevolezza, disattenzione o incuria
   - comportamenti sleali o fraudolenti
   - errore materiale
2) eventi relativi agli strumenti:
   - azione di virus informatici o di programmi suscettibili di recare danno
   - spamming o tecniche di sabotaggio
   - malfunzionamento, indisponibilità o degrado degli strumenti
   - accessi esterni non autorizzati
   - intercettazione di informazioni in rete
3) eventi relativi al contesto fisico-ambientale:
   - ingressi non autorizzati a locali/aree ad accesso ristretto
   - sottrazione di strumenti contenenti dati
   - eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
   - guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
   - errori umani nella gestione della sicurezza fisica

È possibile, per ulteriori dettagli, rinviare a documenti analoghi già redatti in tema di piani di sicurezza e gestione del rischio, come ad es.: Business Continuity Plan, Disaster Recovery Plan, ecc. (si tenga però presente che le analisi alla base di questi altri documenti possono avere una natura ben diversa).
Impatto sulla sicurezza: descrivere le principali conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento, e valutare la loro gravità anche in relazione alla rilevanza e alla probabilità stimata dell'evento (anche

in termini sintetici: es., alta/media/bassa). In questo modo è possibile formulare un primo indicatore omogeneo per i diversi rischi da contrastare.
L'analisi dei rischi può essere condotta utilizzando metodi di complessità diversa: l'approccio qui descritto è volto solo a consentire una prima riflessione in contesti che per dimensioni ridotte o per altre analoghe ragioni, non ritengano di dover procedere ad una analisi più strutturata.

Misure in essere e da adottare (regola 19.4)

Contenuti
In questa sezione vanno riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.
Le misure da adottare possono essere inserite in una sezione dedicata ai programmi per migliorare la sicurezza.

Informazioni essenziali
Misure: descrivere sinteticamente le misure adottate (seguendo anche le indicazioni contenute nelle altre regole dell'Allegato B del Codice).
Descrizione dei rischi: per ciascuna misura indicare sinteticamente i rischi che si intende contrastare (anche qui, si possono utilizzare le indicazioni fornite dall'Allegato B).
Trattamenti interessati: indicare i trattamenti interessati per ciascuna delle misure adottate.
Determinate misure possono non essere riconducibili a specifici trattamenti o banche di dati (ad esempio, con riferimento alle misure per la protezione delle aree e dei locali).
Occorre specificare se la misura è già in essere o da adottare, con eventuale indicazione, in tale ultimo caso, dei tempi previsti per la sua messa in opera.
Struttura o persone addette all'adozione: indicare la struttura o la persona responsabili o preposte all'adozione delle misure indicate.

Ulteriori elementi per la descrizione analitica delle misure di sicurezza (v. anche tab. 4.2)*
Oltre alle informazioni sopra riportate può essere opportuno compilare, per ciascuna misura, una scheda analitica contenente un maggior nume-

* Da indicare facoltativamente.

ro di informazioni, utili nella gestione operativa della sicurezza e, in particolare, nelle attività di verifica e controllo.
Queste schede sono a formato libero e le informazioni utili devono essere individuate in funzione della specifica misura. A puro titolo di esempio, possono essere inserite informazioni relative a:
- la minaccia che si intende contrastare
- la tipologia della misura (preventiva, di contrasto, di contenimento degli effetti ecc.)
- le informazioni relative alla responsabilità dell'attuazione e della gestione della misura
- i tempi di validità delle scelte (contratti esterni, aggiornamento di prodotti, ecc.)
- gli ambiti cui si applica (ambiti fisici – un reparto, un edificio, ecc. – o logici – una procedura, un'applicazione, ecc. –)

Può essere opportuno indicare chi ha compilato la scheda e la data in cui la compilazione è terminata.

Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

Contenuti
In questa sezione sono descritti i criteri e le procedure adottati per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati. L'importanza di queste attività deriva dall' eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci. Pertanto, è opportuno descrivere sinteticamente anche i criteri e le procedure adottate per il salvataggio dei dati al fine di una corretta esecuzione del loro ripristino.

Informazioni essenziali (v. anche tab. 5.1)
Per quanto riguarda il ripristino, le informazioni essenziali sono:
Banca dati/Data base/Archivio: indicare la banca dati, il data base o l'archivio interessati.
Criteri e procedure per il salvataggio e il ripristino dei dati: descrivere sinteticamente le procedure e i criteri individuati per il salvataggio e il ripristino dei dati, con eventuale rinvio ad un'ulteriore scheda operativa o a documentazioni analoghe.
Pianificazione delle prove di ripristino: indicare i tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate.

Ulteriori elementi per specificare i criteri e le procedure per il salvataggio e il ripristino dei dati (v. anche tab. 5.2) *
Data base: identificare la banca, la base o l'archivio elettronico di dati interessati.
Criteri e procedure per il salvataggio dei dati: descrivere sinteticamente la tipologia di salvataggio e la frequenza con cui viene effettuato.
Modalità di custodia delle copie: indicare il luogo fisico in cui sono custodite le copie dei dati salvate.
Struttura o persona incaricata del salvataggio: indicare la struttura o le persone incaricate di effettuare il salvataggio e/o di controllarne l'esito.

Pianificazione degli interventi formativi previsti (regola 19.6)

Contenuti
In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Informazioni essenziali
Descrizione sintetica degli interventi formativi: descrivere sinteticamente gli obiettivi e le modalità dell'intervento formativo, in relazione a quanto previsto dalla regola 19.6 (ingresso in servizio o cambiamento di mansioni degli incaricati, introduzione di nuovi elaboratori, programmi o sistemi informatici, ecc).
Classi di incarico o tipologie di incaricati interessati: individuare le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.
Tempi previsti: indicare i tempi previsti per lo svolgimento degli interventi formativi.

Trattamenti affidati all'esterno (regola 19.7)

Contenuti
Redigere un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

* Da indicare facoltativamente.

Informazioni essenziali
Descrizione dell'attività "esternalizzata": indicare sinteticamente l'attività affidata all'esterno.
Trattamenti di dati interessati: indicare i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività.
Soggetto esterno: indicare la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento).
Descrizione dei criteri: perché sia garantito un adeguato trattamento dei dati è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:
1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Contenuti
In questa sezione vanno rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura – o la separazione fra dati identificativi e dati sensibili –, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti. Questo punto riguarda solo organismi sanitari e esercenti professioni sanitarie (regola 24).

Informazioni essenziali
Trattamenti di dati: descrivere i trattamenti (le banche o le basi di) dati oggetto della protezione
Protezione scelta: riportare la tipologia di protezione adottata, scelta fra quelle indicate dal Codice o in base a considerazioni specifiche del titolare.
Tecnica adottata: descrivere sinteticamente, in termini tecnici ed eventualmente organizzativi, la misura adottata. Ad esempio, in caso di utilizzo di cifratura, le modalità di conservazione delle chiavi e le procedure di utilizzo.

PARTE II - TABELLE

Per ciascuna regola sono riportate, di seguito, una o più tabelle.
Le istruzioni per la compilazione dei campi che le compongono è contenuta nella Parte I.
Per ciascuna tabella può essere indicata facoltativamente anche la data di compilazione, che può rivelarsi utile qualora la tabella sia compilata in data significativamente diversa (antecedente) rispetto alla redazione finale del DPS.

Tabella 1.1 - **Elenco dei trattamenti: informazioni essenziali**

Descrizione sintetica del trattamento		Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati	S	G			

Tabella 1.2 - **Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti**[2]

Identificativo del trattamento	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnessione

[2] Da compilare facoltativamente, collegandola alla tabella precedente, ad esempio attraverso l'identificativo.

Tabella 2 - **Competenze e responsabilità delle strutture preposte ai trattamenti**

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura

Tabella 3 - **Analisi dei rischi**

Rischi		Si/No	Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamenti degli operatori	sottrazione di credenziali di autenticazione		
	carenza di consapevolezza, disattenzione o incuria		
	comportamenti sleali o fraudolenti		
	errore materiale		
	altro evento		
Eventi relativi agli strumenti	azione di virus informatici o di programmi suscettibili di recare danno		
	spamming o tecniche di sabotaggio		
	malfunzionamento, indisponibilità o degrado degli strumenti		
	accessi esterni non autorizzati		
	intercettazione di informazioni in rete		
	altro evento		

Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto		
	sottrazione di strumenti contenenti dati		
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria		
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)		
	errori umani nella gestione della sicurezza fisica		
	altro evento		

Tabella 4.1 - **Le misure di sicurezza adottate o da adottare**

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misura già in essere	Misura da adottare (*)	Struttura o persone addette all'adozione

(*) Indicare eventualmente i tempi previsti per l'adozione delle misure

Tabella 4.2 - **Scheda descrittiva delle misure adottate**[3]

Scheda n.		Compilata da		Data di compilazione	
Misura					
Descrizione sintetica					
Elementi descrittivi					
Data aggiornamento					

[3] Da compilare facoltativamente.

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

Ripristino		
Banca/data base/archivio di dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino

Tabella 5.2 - **Criteri e procedure per il salvataggio dei dati**[4]

Salvataggio			
Banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio

[4] Da compilare facoltativamente.

Tabella 6 - **Pianificazione degli interventi formativi previsti**

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti

Tabella 7 - **Trattamenti affidati all'estero**

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure

Tabella 8 - **Cifratura dei dati o separazione dei dati identificativi** (solo per organismi sanitari ed esercenti professioni sanitarie)

Trattamenti di dati	Protezione scelta (Cifratura/Separazione)	Tecnica adottata	
		Descrizione	Informazioni utili

INDICE

La privacy
Linee guida ad uso delle associazioni di volontariato

Premessa pag. 5
Le parole chiave pag. 5
Elenco dei fac-simile di documento, di seguito riportati, per rispondere a standard minimi di sicurezza dei dati pag. 8
Riepilogo dei principali adempimenti pag. 23
Documento programmatico sulla sicurezza (D.P.S.) pag. 25
Guida operativa per il Documento Programmatico sulla Sicurezza (versione ad uso delle associazioni) pag. 26

Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)
(versione Garante Privacy)

Premessa pag. 31
Parte I - Istruzioni pag. 31
Parte II - Tabelle pag. 39

Stampato su carta riciclata con utilizzo di inchiostri ecologici a base di olii vegetali

a cura di
Scripta Coperco
via Albere 19 - 37138 Verona
tel. 045 8102065 - fax 045 8102064
idea@scriptanet.net