DAVIDE CESTER

# LA PRIVACY NELLE ASSOCIAZIONI DI VOLONTARIATO E NON PROFIT

COLLANA ELEMENTI

# LA PRIVACY NELLE ASSOCIAZIONI DI VOLONTARIATO E NON PROFIT

*Di e a cura dell'Avv. Davide Cester*
*Consulente legale del*
*Centro di Servizio per il Volontariato della Provincia di Padova*

COLLANA ELEMENTI



## PRESENTAZIONE ALLA SECONDA EDIZIONE

Ma la privacy è solo burocrazia? Qual'e l'utilità di tutto questo meccanismo di informative, consensi, documenti, regole, divieti? La solita legge all'italiana piena di obblighi che nessuno rispetta?

Queste alcune delle (giustificate e spesso fondate) domande delle associazioni nel corso di questi tre anni di attuazione del Codice della Privacy.

Questo piccolo aggiornamento del volume edito nel marzo 2005 si propone di indicare le sopravvenute modifiche e novità di legge e di ulteriormente semplificare i problemi e gli adempimenti, alla luce dell'esperienza concreta e delle indicazioni venute dalle decisioni del Garante per la Protezione dei Dati Personali.

Ma al di là delle "carte" e del problema – che purtroppo rimane – di evitare le violazioni che possono avere conseguenze penali o civili o amministrative, a cosa devono puntare le associazioni e cosa è veramente importante?

Certo, esistono campi estranei al *non profit* (la biomedica, il giornalismo, la pubblicità, la giustizia, ecc.) in cui le questioni non sono solo formali: si tratta infatti di volta in volta di decidere in che misura vada tutelata la privacy in rapporto ad altri interessi e principi fondamentali, anche di rango costituzionale (la ricerca scientifica, la libertà di espressione e di cronaca, la libera iniziativa economica, l'accertamento dei reati, ecc.). Sono temi importanti e ancora aperti.

Come trattare i *dati genetici* che permettono di conoscere le caratteristiche non solo dell'individuo ma anche della sua discendenza, o che potrebbero essere utilizzati dalle assicurazioni per valutare il rischio assicurato o dalle aziende per valutare l'assunzione di una persona invece che di un'altra? Come assicurare al tempo stesso la corretta informazione e il rispetto della vita privata e della riservatezza, soprattutto in caso di minori o persone deboli? Come limitare o comunque regolare le "intrusioni" operate giornalmente da chi ci contatta al telefono, via mail o via posta?

Aspetti che coinvolgono l'individuo più che le associazioni o il volontariato.

Ma anche nel mondo del volontariato e del *non profit* c'è spazio per quella che è la sostanza della privacy: uno stile di servizio basato sul rispetto della persona, sull'attenzione e sulla fiducia, sulla capacità di accostarsi e di capire che tipo di "vicinanza" instaurare, e soprattutto di rendere certa la persona che il rapporto con l'ente sarà "fiduciario" e quello con il volontario confidenziale ed esclusivo.

L'Autore



*PRESENTAZIONE ALLA PRIMA EDIZIONE*

*Dal "lontano" 1997 – da quando è entrata in vigore la prima legge italiana sul trattamento dei dati personali – la privacy si è paradossalmente introdotta nelle cassette della posta e nelle case degli italiani, destinatari di "informative" e richieste di "consenso" per i più disparati trattamenti di dati (dati bancari, concorsi a premi, rapporti di lavoro, abbonamenti…), e ha anche impegnato chiunque utilizzi dati personali e informazioni relative a terzi a regolamentare questa attività, adattandola alle prescrizioni della nuova disciplina.*

*L'ultima fatica legislativa è rappresentata dal nuovo "Codice o Testo Unico in materia di protezione dei dati personali", contenuto nel Decreto Legislativo n. 196/03 ed entrato in vigore il 1° gennaio 2004.*

*Le Organizzazioni di Volontariato ed in genere le associazioni e gli enti non profit non sono rimasti estranei alle regole della privacy e, al pari di qualunque soggetto che esegue un trattamento o che lo subisce devono – salvo alcune esenzioni – sottostare a precisi obblighi e sono titolari di determinati diritti.*

*Alcuni adempimenti richiedono il sostenimento di spese non irrilevanti, e comunque una organizzazione interna scrupolosa e attenta.*

*Questa pubblicazione nasce dall'esigenza di risolvere i problemi applicativi della nuova disciplina proprio con speciale riferimento alle organizzazioni di volontariato e al mondo dell'associazionismo.*

*Base del lavoro è stata la guida "privacy, istruzioni per l'uso" che le associazioni hanno precedentemente consultato nel sito del CSV Padova, ma sono stati introdotti molti approfondimenti, esempi, aggiornamenti e nuovi strumenti operativi, secondo un taglio che rimane il più possibile pratico e diretto.*

*Una prima parte – sotto forma di domande/risposte - è dedicata alle questioni e quesiti fondamentali; una seconda ai modelli di documenti che le associazioni devono o possono predisporre; una terza alle norme e ai provvedimenti del Garante. Si è aggiunto anche materiale dedicato agli aspetti più tecnici, e cioè alle misure e ai sistemi informatici che si possono ritenere compatibili con le nuove disposizioni.*

*Il lavoro, dedicato principalmente alle associazioni/organizzazioni di volontariato, contiene esempi e soluzioni molto spesso riferibili anche al mondo più vasto dell'associazionismo (associazioni non riconosciute, associazioni di promozione sociale, ecc.).*

*Auguriamo alle associazioni buon lavoro, con l'auspicio che questo volume di "Elementi" risolva e allevi molti dubbi e difficoltà, ma con l'avvertimento di adeguare di volta in volta quanto esposto e consigliato alla propria particolare realtà associativa.*

*Il Presidente del CSV*
*Giorgio Ortolani*

# IMPORTANTE – ISTRUZIONI PER L'USO

Il tentativo di rendere comprensibili e il più possibile chiare le norme del nuovo "Codice o Testo Unico in materia di protezione dei dati personali" e di spiegarne l'effettiva portata e applicazione in ambito di volontariato e *non profit* cela sicuramente dei rischi non indifferenti.

La disciplina di legge è infatti molto complessa ed estesa, e la sua corretta applicazione può variare da caso a caso, a seconda delle caratteristiche del singolo soggetto che tratta dati personali e del tipo di trattamento di dati effettuato.

Le norme generali del Codice possono poi essere derogate da regole specifiche relative a settori determinati, come ad esempio l'ambito sanitario, o giudiziario, o pubblico, o relativo ai rapporti di lavoro, la cui approfondita analisi necessariamente esula dal contenuto di questo lavoro.

**Le risposte, i commenti, gli esempi ed i modelli riportati costituiscono quindi dei criteri di massima e vanno sempre valutati con riferimento alla propria realtà associativa**.

Inoltre, lo studio della legge e gli adempimenti che essa richiede presuppongono un costante ed attento **aggiornamento**, poiché il legislatore italiano da una parte ha mostrato più volte, nel corso di questi anni, di voler migliorare, semplificare ed integrare la disciplina; dall'altra, con riferimento alle cd. "misure di sicurezza" informatiche, ne ha più volte differito i tempi di attuazione e comunque ne prevede la modifica in ragione delle modifiche tecnologiche e informatiche.

L'applicazione del Codice richiede anche la capacità di interpretare norme e concetti tecnici non semplici, soprattutto nel caso di trattamento elettronico dei dati; per questo si è inserita nel lavoro anche una "scheda tecnica" che analizza le varie possibilità di intervento sui sistemi informativi utilizzati per il trattamento dei dati, e la parte relativa alle misure di sicurezza e protezione è stata arricchita di esempi e spiegazioni tecniche raccolte da esperti del settore informatico.
Di molto aiuto sono inoltre le pronunce interpretative e le decisioni del Garante per la Protezione dei Dati Personali, cui si farà spesso cenno.



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

Il lavoro è disponibile in forma di FAQ e quale pubblicazione nel sito del Centro di Servizio per il Volontariato della Provincia di Padova www.csvpadova.org.

## ATTENZIONE



Padova, 1 maggio 2008

# DOMANDA E RISPOSTA: I QUESITI PIÙ IMPORTANTI

*Si riportano qui di seguito 28 domande/risposte sugli articoli del Codice o Testo Unico sul trattamento dei dati personali (che per comodità chiameremo anche solo "Codice") sulle questioni più rilevanti e sulle ricadute concrete della disciplina per le associazioni di volontariato (Odv) e di promozione sociale (Aps), e in generale per le associazioni non profit. Le norme del codice sono spesso riportate in riquadri; i commenti e gli esempi sono scritti in corsivo.*

## 1. Qual'è la legge sulla privacy?

La disciplina sulla privacy è contenuta nel Decreto Legislativo n. 196/03, detto "Testo Unico" o "**Codice in materia di protezione dei dati personali**"[1], entrato in vigore il 1° gennaio 2004. Il Codice raccoglie, le disposizioni della "vecchia" Legge n. 675/96 (che è stata abrogata), le leggi successive e i regolamenti attuativi. Il testo della legge è disponibile nel sito del Garante per la Protezione dei Dati Personali *www.garanteprivacy.it* oppure in altri siti come *www.privacy.it*

* * *

## 2. Definizioni

Per comprendere le norme sulla privacy è necessario avere un minimo di familiarità con i seguenti concetti/definizioni contenuti nell'art. 4 del Codice:

**Trattamento** è "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,

[1] D. Lgs. 30.6.2003 n. 196 pubblicato sulla Gazzetta Ufficiale n. 174 del 29.7.2003, suppl. ordinario n. 123.



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

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".

**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".

**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".

**Incaricati** sono "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile". L'incaricato "opera sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite".

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

**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.

**Comunicazione dei dati** è "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato […], dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

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

## 3. Qual è lo scopo del Codice della privacy?

Il Codice vuole garantire che il trattamento dei dati personali, e cioè l'utilizzo delle informazioni e notizie che riguardano una persona (fisica o giuridica), 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 (art. 2)

Più precisamente, il Codice si propone soprattutto di far sì:

a) che i dati personali vengano utilizzati per **scopi leciti** e comunque per le **finalità** in base alle quali sono stati raccolti;
b) che i dati personali non vengano conosciuti da estranei, che non vengano diffusi **o comunque utilizzati contro la volontà o nell'ignoranza della persona o dell'ente cui si riferiscono**;
c) che i dati personali non vengano distrutti o perduti.

*La privacy (cui corrispondeva inizialmente il concetto italiano di "riservatezza") nasce in Inghilterra intesa quale "diritto ad esser lasciati soli", cioè a non subire illegittime intrusioni nella propria vita privata.*

*Nel mondo attuale, in cui le informazioni che ci riguardano (nominativo, indirizzo, numero di telefono, abitudini, acquisti, stato di salute, iscrizioni a enti o partiti, ecc.) vengono da noi stessi direttamente o indirettamente comunicate a molti soggetti, il concetto di privacy e la tutela di legge si è progressivamente allargata al diritto di decidere quali informazioni vogliamo rendere pubbliche o comunque vogliamo siano conosciute da terzi e da quali terzi (cd.* diritto all'autodeterminazione informativa*), e soprattutto al* ***diritto a che i nostri dati siano utilizzati solo per le finalità e nell'ambito nel quale li abbiamo comunicati, nel rispetto della legge e senza che ne derivi una violazione della nostra dignità, identità e riservatezza*** *(cd. diritto alla protezione dei dati personali).*





## 4. Quali dati trattano le associazioni e che natura hanno?

Le Odv e in genere la associazioni non profit raccolgono e utilizzano comunemente, nello svolgimento della loro attività, dati personali, e cioè informazioni e notizie riferite:

a) ai propri soci/aderenti;
b) ai beneficiari dell'attività istituzionale o utenti del servizio;
c) ai consulenti e collaboratori esterni;
d) agli eventuali dipendenti;
e) agli enti pubblici;
f) agli altri enti *non-profit* e in genere i soggetti con cui vengono a contatto;
g) alle persone, enti e aziende a cui indirizzare campagne di sensibilizzazione e *fundraising*, ecc.

*Costituiscono per esempio* ***raccolte cartacee*** *di dati personali il libro dei soci, il libro dei volontari, la rubrica per la corrispondenza, l'elenco dei donatori, i bilanci, le convenzioni, ecc. Tali dati possono anche essere gestiti tramite computer e contenuti in* ***banche dati****, situazione che richiede l'adozione di particolari misure di sicurezza e di protezione dei computer* [2]*.*

Quanto alla natura dei dati, si possono distinguere:

→ **DATI COMUNI** (es. il nominativo, la data di nascita, il numero di cellulare dei soci/volontari o beneficiari, l'avvenuto versamento della quota associativa, gli studi compiuti)[3], alcuni dei quali sono **PUBBLICI**, e cioè ricavati o comunque ricavabili da albi, elenchi e registri che per legge sono pubblici (es. il codice fiscale o le liste elettorali).

→ **DATI SENSIBILI** [4]

→ **DATI GIUDIZIARI** [5]

[2] Cfr. D/R n. 17ss.
[3] Non esiste nel Codice una esplicita definizione di **dato comune**. Saranno comuni, pertanto, tutti quei dati non compresi nelle altre categorie definite dal Codice (dati sensibili, giudiziari, genetici, sanitari, anonimi, ecc..). E' importante ricordare, in ogni caso, che anche il nome e il cognome possono perdere la loro natura di "dati comuni" e diventare "dati sensibili" quando idonei a rivelare l'adesione ad associazioni religiose, filosofiche, politiche o sindacali (cfr. D/R n. 12).
[4] Cfr. D/R. n. 12.
[5] Cfr. D/R n. 16.

*Si deve ritenere che costituiscano dati personali (comuni o sensibili) anche le **immagini**, i suoni, i filmati, gli MMS ecc., quando consentono di individuare una persona determinata. Anche a tali dati, quindi si applicano le regole del Codice della Privacy, oltre alle norme del codice civile (art. 10) sulla tutela dell'immagine.*

* * *

## 5. Il Codice riguarda anche le associazioni *non profit*? Si devono considerare "titolari del trattamento"?

**Assolutamente SI**, buona parte delle norme generali del Codice si applicano anche alle organizzazioni/associazioni di Volontariato e in genere agli enti *non profit*, che sono "titolari del trattamento" se e ogni qualvolta svolgono anche una sola delle operazioni che concretano un trattamento di dati personali [6].

Il Codice, infatti non si applica solo ai trattamenti di dati svolti da "persone fisiche per fini esclusivamente personali" (es. rubrica telefonica nella propria abitazione) e sempre che non si svolga una comunicazione sistematica o diffusione (art. 5, comma 3).

Il trattamento di dati svolto da una associazione di volontariato o comunque da un ente *non profit* non ha fini esclusivamente personali, comporta molte volte una comunicazione sistematica, e rientra pertanto nell'ambito di applicazione delle norme del Codice, ed in particolare di tutte le norme dedicate agli enti privati, quali sono le associazioni e le fondazioni.

**Titolare del trattamento**, quando questo è svolto da una persona giuridica (qual è l'associazione), è "l'entità nel suo complesso" (art. 28), e cioè **l'associazione/organizzazione**, e non le persone fisiche che ne fanno parte[7].

[6] Cfr. le "definizioni" (D/R n. 2).

[7] Ciò non toglie:
- che le decisioni sui trattamenti da svolgere vanno adottate dall'organo o dalle persone fisiche cui è attribuita la gestione dell'ente (es. Consiglio Direttivo, il Presidente, un Consigliere);





*E' utile precisare che, ai fini dell'applicazione del Codice, non è rilevante l'iscrizione dell'associazione al registro del volontariato ex L. 266/91 o al registro della promozione sociale ex L. 383/00 o all'anagrafe delle ONLUS ex D.Lgs. 460/97: le norme del Codice che si riferiscono alle associazioni e agli enti non profit, infatti, non distinguono tra i vari soggetti appartenenti al terzo settore, ma parlano genericamente di "associazioni, enti o organismi senza scopo di lucro".*

L'art. 28 infine stabilisce che debba esser considerato titolare del trattamento anche **la sezione locale o l'organismo periferico di una associazione**, qualora essa eserciti "un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza".

*Se quindi la sezione/organismo locale di una associazione nazionale decide in autonomia in tema di privacy rispetto ala "casa madre", va considerata "titolare", e cioè soggetto autonomo ai fini dell'applicazione del Codice e del rispetto degli obblighi conseguenti: deve pertanto predisporre una propria informativa, deve chiedere il consenso al trattamento, deve redigere se del caso un proprio Documento Programmatico sulla Sicurezza e così via[8].*

- che gli adempimenti richiesti dal Codice devono ovviamente essere attuati da persone fisiche (ad es. il Presidente, un consigliere delegato, i dipendenti, o anche i volontari), che saranno nominati Responsabili (cfr. D/R n. 11) o Incaricati del trattamento (cfr. D/R n. 21);
- che i limiti imposti dalla legge vanno rispettati da chiunque dell'associazione utilizzi dati personali;
- che, infine, le responsabilità civili, amministrative e penali in caso di violazione del Codice gravano prevalentemente sulle persone fisiche che hanno agito (cfr. n. 25).

[8] Cfr. D/R seguenti.

## 6. Quali sono i criteri, i limiti e le finalità con cui le associazioni devono trattare i dati personali?

Ai sensi dell'art. 11 del Codice gli enti *non profit*, come qualsiasi titolare:

- devono trattare i dati in modo lecito e secondo correttezza;
- possono raccogliere e registrare i dati solo per scopi determinati, espliciti e legittimi, ed utilizzare i dati in altre operazioni del trattamento in termini compatibili con tali scopi;
- devono assicurarsi che siano esatti e, se necessario, aggiornati, e che siano pertinenti, completi e non eccedenti rispetto alle finalità per cui sono stati raccolti;
- devono conservarli per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti.

Il PRINCIPIO DI FINALITÀ è uno dei fondamenti della privacy.

Significa che **la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate all'interessato e poi rispettate**.

Per le associazioni *non profit* le finalità del trattamento dei dati generalmente coincidono o sono compresi negli **scopi istituzionali indicati nello statuto**[9].

*Quindi ad esempio quando l'associazione raccoglie i dati comuni dei suoi associati per inserirli nel libro soci, per inviare a casa la corrispondenza o il giornalino dell'associazione e comunque per averne la reperibilità, o raccoglie i dati dei beneficiari dell'attività per garantire il servizio,* ***non potrà senza l'autorizzazione e/o l'informazione specifica ai soci/beneficiari usare tali dati per scopi diversi da quelli istituzionali****: ad esempio non potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per pubblicità, iniziative commerciali o per propaganda elettorale* [10]*o comunque per scopi che non riguardano l'ente.*

[9] Anche se spesso lo statuto è spesso generico, ed invece le finalità del trattamento vanno maggiormente specificate nell'informativa: cfr. D/R n. 9.

[10] Cfr. risposta del Garante 9.10.2000 in www.garanteprivacy.it/provvedimenti.



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

**In caso di trattamento di DATI SENSIBILI, SANITARI e GIUDIZIARI, l'utilizzo per fini diversi da quelli indicati nello statuto è invece del tutto vietato all'associazione**[11].

[11] Cfr. D/R n. 13, 15 e 16.

## 7. I dati vanno aggiornati? Possono essere conservati?

L'**aggiornamento dei dati**, deve essere svolto quando è necessario per il corretto raggiungimento delle finalità del trattamento o per soddisfare una legittima esigenza dell'interessato.

*Chiaramente è interesse dell'associazione far sì che le informazioni relative ai soggetti con cui e a favore di cui opera siano aggiornati, e nella pratica ciò avviene comunemente, per iniziativa dell'associazione o dell'interessato che comunica all'associazione le variazioni intervenute (es. cambio di indirizzo). L'aggiornamento dei dati è anche un vero e proprio diritto dell'interessato* [12].

Quanto al problema della **conservazione dei dati**, ci si può chiedere se l'associazione possa trattenere e utilizzare i dati personali dei propri associati anche dopo che essi hanno lasciato l'associazione[13]. L'art. 11 impone per la verità di **cancellare** i dati, poiché il socio non fa più parte dell'associazione e quindi ha diritto che essa non utilizzi più il suo nome e i suoi dati e di non risultare più socio. Un trattamento "successivo" richiede quindi apposita autorizzazione dell'ex socio a che l'associazione conservi il suo nome e i suoi dati, o lo contatti periodicamente, o invii materiale via posta o via mail.

*Qualora le esigenze dell'associazione siano quelle di conservare solamente una sorta di "**albo d'oro**" di coloro che sono stati soci, tale operazione può probabilmente essere attuata attraverso una rubrica cartacea conservata in luogo non accessibile a terzi: in questo caso, il trattamento potrebbe esser considerato svolto "per fini esclusivamente personali", come richiesto dall'art. 16 del Codice, sempre che, però i dati non siano comunicati a terzi o diffusi:*

*Quello della conservazione dei dati dopo la cessazione del rapporto associativo è un aspetto delicato, poiché, le informazioni da cui emerge l'appartenenza ad una associazione possono essere considerate "sensibili", se idonee "a rivelare l'adesione ad associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale"* [14]*. Si capisce che la diffusione o la comunicazione a terzi di una precedente iscrizione ad una di queste associazioni*[15]*, o in genere ad una associazione, di una persona che ad un certo punto ha deciso di non farne più parte potrebbe essere considerata illecita e comunque non gradita all'interessato.*

[12] Cfr. D/R n. 10.
[13] Si tratta di un'esigenza sentita dalle associazioni, che desiderano anche solo conservare traccia di coloro che hanno "transitato" all'interno dell'ente.
[14] Cfr. D/R n. 12.
[15] Anche se non molte associazioni di volontariato e di promozione sociale possono ritenersi a "carattere religioso, filosofico, politico o sindacale".



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

## 8. Le associazioni ed enti *non profit* devono notificare al Garante l'esistenza del trattamento?

I titolari di un trattamento devono notificare (e cioè comunicate in via elettronica) al Garante per la Protezione dei Dati Personali il fatto di svolgere un trattamento di dati personali **solo nei casi specificamente indicati dall'art. 37 del Codice**.

Per quanto riguarda il *non profit*, hanno l'obbligo di notificazione le "associazioni, enti o organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale" che trattano "dati idonei a rivelare la vita sessuale o la sfera psichica" (art. 37, lett. c).

*Questo articolo non è del tutto chiaro e usa concetti abbastanza vaghi per identificare i soggetti tenuti all'adempimento di un obbligo così preciso e anche gravoso.*

Il Garante per la Protezione dei dati personali, con parere del 23.4.2004, ha però precisato che l'elenco degli enti di cui all'art. 37, lett. c) è tassativo e non esemplificativo, e che "**non** vanno notificati i trattamenti effettuati da associazioni, enti o organismi che **non** hanno carattere politico, sindacale, religioso o filosofico, come ad esempio cooperative che svolgono attività di ricovero e assistenza a malati psichici".

Se quindi secondo il Garante sono esentate dalla notifica le cooperative di tipo A, per non aver esse carattere politico, sindacale, religioso o filosofico, **non hanno probabilmente alcun obbligo di notifica anche tutte le Odv e Aps che per statuto non presentano una chiara connotazione politica, sindacale, religiosa o filosofica, e che per esempio si richiamano genericamente a doveri e principi di solidarietà e altruismo**[16].

**Ovviamente non hanno alcun obbligo di notifica le associazioni che non trattano** dati idonei a rivelare la **vita sessuale** o la **sfera psichica**.

[16] Di opinione contraria, ma in uno scritto forse antecedente alla decisione del Garante richiamata, sembrano R. e R. IMPERIALI, *Privacy: gli obblighi di notificazione al Garante*, in *Terzo Settore, Il Sole 24 Ore*, n. 4/04, p. 35.

*Qualora in base a quanto detto sopra, una associazione si ritenga "a rischio notifica", è consigliabile acquisisca un parere specifico da un esperto, per un approfondimento della sua posizione e per acquisire informazioni sulle modalità della notifica, che deve avvenire per via telematica.*

Si ricordi che la notifica, se dovuta, andava compiuta entro il "lontano" **30 aprile 2004** (art. 181 del Codice) e che la mancata, ritardata o incompleta notifica potrebbe comportare, ai sensi dell'art. 163, "l'applicazione della sanzione amministrativa del pagamento di una somma da € 10.000 a € 60.000"[17].

[17] Cfr D/R n. 25.





## 9. Le associazioni devono fornire all'interessato l'informativa ex art. 13 del Codice?

**Assolutamente SI**, l'informativa costituisce il principale obbligo in capo a chi svolge un trattamento di dati personali. L'informativa è una **comunicazione** che serve per far conoscere all'interessato come il titolare gestisce e utilizza i dati che lo riguardano. E' inoltre il presupposto essenziale perché l'interessato possa dare il consenso/autorizzazione al trattamento, quando questo è richiesto dalla legge.

L'informativa è prevista dall'art. 13 del Codice:

> L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
> a) le finalità e le modalità del trattamento cui sono destinati i dati;
> b) la natura obbligatoria o facoltativa del conferimento dei dati;
> c) le conseguenze di un eventuale rifiuto di rispondere;
> d) 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;
> e) i diritti di cui all'articolo 7;
> f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile […]
> L'informativa contiene […] può non comprendere gli elementi già noti alla persona che fornisce i dati […].
> Se i dati personali non sono raccolti presso l'interessato, l'informativa […] è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

L'art. 13 dice che l'informativa può essere anche **orale**; tuttavia, poiché il titolare dovrà comunque dimostrare di averla fornita, è evidente che una qualche **forma scritta** è consigliabile.

*L'informativa (insieme al consenso, ove richiesto) costituisce per le associazioni, soprattutto le più piccole, un'incombenza burocratica e scomoda. E' utile però tener presente che:*

- *per quanto riguarda i **nuovi soci**, l'informativa può **essere allegata o scritta sulla domanda di adesione all'associazione**[18]. Se è prevista una firma del modulo da parte dell'aspirante socio, la firma varrà anche come "presa visione" dell'informativa. In ogni caso la compilazione del modulo (nel quale è stampata anche l'informativa) direttamente da parte del socio è da considerarsi sufficiente;*
- *l'informativa può essere anche spedita **via fax o via e-mail**. Del fax è consigliabile conservare la ricevuta di avvenuto invio (meglio ancora se l'interessato lo rispedisce firmato). Dell'e-mail può essere opportuno chiedere al destinatario di rinviare un messaggio di "conferma", che l'ente potrà stampare e conservare;*
- *l'informativa **vale per tutti i trattamenti futuri** che riguardano l'interessato, e va quindi **fornita una sola volta**, se il trattamento dei dati non cambia e rispetta le finalità indicate nell'informativa medesima;*
- *l'informativa **deve essere comunicata solo a quei soggetti dei quali l'associazione raccoglie, registra o utilizza i dati**, e tra costoro non rientrano quindi i beneficiari dell'attività istituzionale che l'ente non identifica[19].*

I **modelli/esempi di informativa** che si propongono[20] sono ovviamente generici e vanno compilati e modificati in base alle caratteristiche dell'associazione e alle modalità del trattamento.

L'informativa va comunicata/consegnata ai **soci e/o volontari**, ai **collaboratori esterni**, ai **dipendenti**, ai **beneficiari e a tutti coloro di cui l'associazione acquisisce, conserva e utilizza dati personali**, che si possono definire "interessati"[21].

[18] In tal senso anche il Garante, che, in relazione ad un trattamento di dati sensibili di un'atleta da parte della sua società sportiva, ha segnalato "*l'opportunità che tali adempimenti vengano compiuti in sede di tesseramento, **oralmente** o, più opportunamente, attraverso la predisposizione di un **apposito modulo** a stampa da fornire a ciascun interessato al momento dell'iscrizione. Vanno infatti salvaguardati i principi di cui agli artt. 10 e 11 della legge* [ora art. 13 del Codice], *secondo cui l'interessato deve essere effettivamente informato, in via preventiva, specie sulle finalità e modalità del trattamento, sull'ambito di diffusione dei dati e sui diritti spettanti ai sensi dell'art. 13* [ora art. 7 del Codice], *anche al fine di poter esprimere un consenso libero e consapevole. Un mero inserimento dell'informativa nei c.d. regolamenti federali non permetterebbe agli interessati di rilevare con evidenza ed immediatezza le informazioni essenziali sul trattamento dei dati personali, informazioni che il legislatore impone di rendere note all'interessato in maniera chiara, in modo da rendere consapevole l'eventuale atto con cui l'interessato stesso autorizza il loro utilizzo e da agevolare il successivo controllo sempre da parte dell'interessato*" (Provvedimento 22.6.1998 in **www.privacy.it** link "Garante" – "Risposte a istanze, quesiti e ricorsi" o **www.garanteprivacy.it**).

[19] Ad es. i pazienti dell'ospedale beneficiari dell'assistenza o delle attività ludiche, salvo ovviamente che l'associazione non acquisisca anche i loro nomi e in genere i loro dati.

[20] Cfr. modello/esempio I (informativa per volontari e/o soci), II (informativa per beneficiari e terzi) e III (informativa per dipendenti e collaboratori).

[21] Cfr. la "definizioni" alla D/R n. 2.





La comunicazione/consegna va fatta nel momento appena precedente a quello in cui l'interessato fornisce i suoi dati all'associazione: in pratica la prima volta che la persona viene a contatto con l'associazione. Se i dati non sono forniti dall'interessato ma da altre persone/soggetti, l'obbligo dell'informativa all'interessato va adempiuto nel momento in cui l'associazione registra i dati o li comunica per la prima volta a terzi.

*Esigenza di molte associazioni (soprattutto quelle con un elevato numero di soci e con un rapido turn-over) è quella di stampare un'unica informativa e renderla pubblica attraverso l'**affissione** nei locali dell'associazione. Si tratta di una scelta non espressamente ammessa dal Codice, che prevede forme semplificate di informativa solo in casi specifici o in ragione di un apposito provvedimento del Garante. L'affissione può costituire elemento presuntivo da cui desumere che l'informativa è pervenuta agli interessati; tuttavia potrebbe tutt'al più "coprire" alcuni soci (quelli che si recano in sede), ma non i beneficiari ed in genere le persone che non accedono alla sede dell'associazione. **Si sconsiglia** pertanto di adottare questa forma.*

*Si deve ritenere allo stesso modo **non corretto l'inserimento dell'informativa nello statuto dell'associazione** (le cui modifiche oltretutto sono decise dall'assemblea con maggioranze particolari, con evidenti problemi nel caso il trattamento di dati si svolga poi in termini diversi da quelli inizialmente descritti).*

*Maggiore idoneità potrebbe avere l'inserimento/pubblicazione dell'informativa **all'interno del giornale/notiziario dell'associazione** (o allegata allo stesso), se fatto pervenire direttamente agli associati[22]. Va precisato che ai sensi dell'art. 13 del Codice l'informativa andrebbe comunicata/consegnata nel momento appena precedente a quello in cui l'interessato fornisce i suoi dati all'associazione, e che pertanto la pubblicazione nel giornalino potrebbe essere considerata tardiva. Tuttavia, nel caso in cui l'associazione non abbia finora comunicato alcuna informativa, tale modalità potrebbe rappresentare se non altro una "sanatoria" per regolarizzare la situazione.*

**ATTENZIONE**: all'informativa va accompagnata la **richiesta di autorizzazione/consenso al trattamento dei dati** in tutti i casi in cui, come si vedrà, questa è considerarsi obbligatoria.

[22] Si consiglia in questo caso di conservare presso la sede traccia dei nominativi dei destinatari o, ancora meglio, se per la spedizione si utilizzano esterni, copia della comunicazione con cui si indicano allo spedizioniere i destinatari medesimi.

## 10. Quali sono i diritti degli interessati nei confronti dei titolari che trattano i dati?

L'art. 1 del Codice afferma che "chiunque ha diritto alla protezione dei dati personali che lo riguardano in conformità alle disposizioni del presente Codice".

La protezione dei dati è assicurata anche attraverso l'esercizio dei diritti indicati dall'art. 7.

In base all'art. 7 **l'interessato può infatti chiedere al titolare** (e quindi all'associazione):
di confermare l'esistenza presso di essa dati personali che lo riguardano e, se esistenti, di comunicarli;
di indicare l'origine dei dati (cioè come e da chi l'associazione li ha acquisiti), le finalità e le modalità del trattamento (cioè perché e come vengono usati i dati, se vengono conservati, se vengono comunicati ad altre persone o enti, con che strumenti elettronici vengono gestiti, ecc.), la denominazione e i dati identificativi (es. sede) dell'associazione quale titolare e i nomi dei soggetti che sono stati designati dall'ente come responsabili o incaricati;
di aggiornare, rettificare o integrare i dati (es. cambio di indirizzo o dello stato civile) , di correggerli in caso siano errati, di cancellare, trasformare in forma anonima o bloccare i dati trattati in violazione di legge;
di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono motivi legittimi (cioè particolari e valide ragioni, ad esempio se ha presentato domanda di recesso dall'associazione, o se il trattamento, anche senza colpa per il titolare, risulta lesivo della sua dignità o riservatezza);
di opporsi al trattamento ai fini dell'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale[23].

[23] Il potere di opposizione non sembra toccare le Odv nel caso esercitino solo le attività cd. marginali di cui all'art. 8 L. 266/91 e con i limiti del D.M. 25.5.1995. Non sembra inoltre applicabile nel caso l'Odv o comunque l'ente *non profit* tratti i dati per l'invio di semplice materiale informativo che si riferisce alla sua attività istituzionale/ideale. Naturalmente l'interessato può opporsi che l'associazione comunichi i suoi dati a terzi per lo svolgimento delle attività indicate dalla norma (invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione





Quindi **ogni persona o ente può chiedere ad ogni titolare** (es. banca, datore di lavoro, azienda, ente pubblico o privato, Odv/Aps, Onlus, ecc.) **se e in che modo utilizza suoi dati personali, e anche le Odv, quali titolari, potrebbero ricevere tale richiesta**.

La richiesta potrà pervenire all'associazione tramite lettera raccomandata, fax o posta elettronica, e anche oralmente nei primi due casi sopra indicati. Una stessa richiesta può essere compiuta dall'interessato anche ripetutamente, ma con un intervallo di tempo di almeno 90 giorni. Inoltre, se l'interessato fa la sua richiesta e l'associazione non detiene suoi dati personali, può chiedere all'interessato un contributo/spese che non ecceda i costi effettivamente sopportati per la ricerca medesima.

Si ricordi che sono **"interessati" anche gli associati/volontari**, e non solo i soggetti esterni all'associazione. Nonostante il silenzio del Codice, si deve ritenere che, se l'interessato è minorenne i diritti possano essere esercitati da chi ha la rappresentanza legale, e cioè i genitori che hanno la potestà, o il tutore se esiste.

*L'esercizio dei diritti degli interessati è un onere importante a carico delle associazioni, e il Garante si è più volte occupato[24] di ricorsi presentati da interessati/soci che avevano esercitato i diritti di cui all'art. 13 nei confronti dell'associazione di appartenenza, ma ritenevano di non aver ottenuto adeguata o tempestiva risposta. In tali casi il Garante, accertato che il ricorso era fondato, ha imposto all'associazione, oltre ad una attività corrispondente alle richieste dell'interessato, il pagamento delle spese del procedimento (art. 150, comma 3 del Codice). Le richieste dell'interessato possono essere dirette anche al Responsabile del trattamento, se nominato[25]; in alternativa, si consiglia comunque all'associazione di individuare una persona/Incaricato[26] cui attribuire il compito di evaderle.*

Infine, è importante ricordare che **i diritti di cui all'art. 7 possono essere esercitati anche da ogni associazione nella qualità di "interessato", con riferimento al trattamento dei dati relativi all'associazione svolto da altri soggetti o enti**. Infatti, in base all'art. 1 del Codice, il diritto alla protezione dei dati personali è attribuito a

commerciale), ma tale comunicazione sarebbe comunque vietata all'Odv, se svolta con finalità del tutto estranee a quelle per le quali i dati sono stati raccolti (cfr. D/R n. 6).
[24] Cfr. ad esempio decisioni del 23.5.2002 e 20.3.2002, in **www.privacy.it** link "Garante" – "Risposte a istanze, quesiti e ricorsi".
[25] Cfr. D/R n. 11.
[26] Cfr. D/R n. 21.

"chiunque", e cioè non solo alle persone fisiche, ma anche alle persone giuridiche, e quindi anche alle associazioni ed enti *non profit* in genere.

* * *

## 11. E' necessario nominare un responsabile del trattamento?

La nomina di un Responsabile del trattamento è una **facoltà e non un obbligo**.

Il Responsabile è "preposto dal titolare al trattamento dei dati personali" (art. 4) ed è scelto tra persone con "esperienza, capacità e affidabilità" anche in relazione al "profilo relativo alla sicurezza". I compiti del responsabile sono individuati per iscritto dal titolare (art. 29).

*Il Responsabile sarà generalmente una persona esperta o che si occupa dei trattamenti mediante computer e vigila sulle misure di sicurezza da adottare, eventualmente in collaborazione con l'Amministratore di sistema*[27]*. Possono essere nominati Responsabili anche più persone, e anche una persona giuridica. La nomina di Responsabili si rivela utile nelle grandi strutture/aziende, nell'ambito di una divisione dei compiti o dei settori di attività, per attribuire ad un solo o a più soggetti i compiti in materia di privacy (Responsabile o Responsabili interni), oppure nei casi in cui l'impresa decide di affidare o appaltare a soggetti o imprese esterne determinate attività che prevedono un trattamento di dati personali: il soggetto o l'impresa esterna potranno in tale caso esser nominati Responsabili (esterni)*[28]*.*

Il Responsabile ha mansioni interne e anche una visibilità esterna, nei confronti degli interessati e del Garante; ad esempio può essere destinatario delle richieste ex art. 7 o può essere richiesto dal Garante ex art. 157 di fornire informazioni o esibire documenti. Il suo nominativo deve essere reso noto all'interessato nell'informativa.

[27] Sempre non siano la stessa persona. Sull'Amministratore di Sistema cfr. D/R n. 19.
[28] Anche le Odv potrebbero probabilmente inserirsi in questo "sistema privacy", nel caso svolgano un trattamento in stretta collaborazione con enti pubblici nell'ambito di un rapporto di convenzionamento; cfr., sul punto, D/R n. 27.





*Nelle associazioni la nomina del Responsabile può servire per "sgravare" il Presidente o l'organo direttivo di incombenze tecniche e organizzative. Responsabile può essere nominato il Presidente, un membro del Consiglio Direttivo, un socio, 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, Aps, ecc.) o della persona fisica che ha eventualmente 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*[29]*.*

Si propone un **modello/esempio di nomina del responsabile**, anche questo da adattare alla situazione concreta[30].

Non è facoltativo ma obbligatorio, invece, individuare all'interno dell'associazione tutti i soggetti o le categorie di soggetti che trattano i dati, e nominarli **"Incaricati" del trattamento** (cfr. n. 21).

[29] Cfr. D/R n. 25.
[30] Cfr. modello/esempio IV (nomina del Responsabile).

## 12. Cosa sono i dati sensibili?

I dati sensibili sono i dati "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 o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 4, lett. d).

I dati sensibili riguardano la sfera più intima dell'individuo e pertanto richiedono una particolare protezione, o perché dati che il soggetto ha interesse a non diffondere o perché informazioni che, se apprese al di fuori di un determinato contesto, possono essere causa di atteggiamenti discriminatori.

***Le Odv e gli enti non profit possono facilmente avere a che fare con dati sensibili****: quelli dei beneficiari dell'attività sociale, quando operano proprio nei settori che il legislatore considera più delicati, come ad esempio l'ambito sanitario e della salute (ad es. chi lavora con malati, soggetti portatori di handicap o tossicodipendenti, ma anche con anziani portatori di patologie), l'ambito religioso o caratterizzato ideologicamente in senso politico, ma anche filosofico (ad es. un'associazione espressamente e "istituzionalmente" pacifista o antiproibizionista), l'ambito dell'appartenenza etnica (es. associazioni che lavorano con i nomadi o extracomunitari).*

Ma, in base all'art. 4 del Codice, si deve ritenere che la stessa **notizia/informazione dell'iscrizione/appartenenza ad una associazione** in qualità di socio/volontario, quando l'associazione presenta "carattere religioso, filosofico, politico o sindacale", costituisce un dato sensibile[31].

[31] In sintonia con quanto precisato dal Garante a proposito dell'obbligo di notifica (cfr. D/R n. 8), si deve ritenere che l'elenco sia tassativo, e che pertanto il nome e cognome di aderenti ad associazioni siano da considerare dati "sensibili" solo se le associazioni presentano carattere religioso, filosofico, politico e sindacale, mentre abbiano natura "comune" se l'associazione si richiama genericamente a doveri e principi di solidarietà e altruismo. Se però si accettasse una interpretazione estensiva dell'articolo 4 si dovrebbe considerare dato sensibile l'adesione o la partecipazione a qualunque associazione, in quanto comunque "idonea a rivelare le convinzioni religiose, filosofiche o di altro genere". Probabilmente, però, si tratta di un'interpretazione troppo forzata, e contraria al sistema del Codice (non avrebbe senso, infatti, l'esonero dall'obbligo di richiedere il consenso di cui all'art. 26, comma 4, lett. a, limitato solamente alle associazioni con carattere religioso, filosofico, politico o sindacale). In ogni caso è bene che le Odv ed in genere le associazioni considerino le banche dati contenenti i nominativi dei propri soci con particolare attenzione.





*Questa tesi sembra confermata dal Garante, che nel provvedimento 27.3.1998 riguardante la tenuta da parte di una associazione a carattere culturale e sindacale di un indirizzario per la trasmissione di un periodico mensile mediante abbonamento postale, ha stabilito che i dati contenuti nell'indirizzario (nome e indirizzo) dovevano essere considerati "sensibili", perché il periodico veniva spedito non a chi semplicemente lo richiedeva (anche esterno all'associazione), ma solo ad iscritti all'associazione, e quindi l'elenco dei destinatari consentiva di identificare tutte le persone che aderivano all'associazione sindacale.*

Sono stati considerati dati sensibili dal Garante anche l'iscrizione ad un partito politico, la diagnosi da infezione da HIV; il referto di non idoneità sportiva, ecc.

## 13. Le associazioni devono chiedere il consenso all'interessato per il trattamento dei suoi dati personali "comuni" e "sensibili"?

Gli art. 23 e 26 del Codice stabiliscono la regola generale per cui il Titolare che tratti dati comuni o sensibili deve acquisire il consenso/autorizzazione dell'interessato:

> Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il CONSENSO ESPRESSO dell'interessato.

> I dati sensibili possono essere trattati solo con il CONSENSO SCRITTO dell'interessato. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Tuttavia, il Codice prevede che il **CONSENSO NON È NECESSARIO**:

> quando il trattamento di dati comuni, con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti o 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 all'atto dell'informativa ai sensi dell'art. 13 (art. 24 comma 1)

> quando il trattamento di dati sensibili è svolto da associazioni, enti o organismi senza scopo di lucro a carattere politico, filosofico religioso o sindacale per il perseguimento dei legittimi scopi statutari, e riguarda dati sensibili di aderenti e soggetti che hanno contatti stabili con l'associazione, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13" (art. 26)



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

Queste norme consentono di ritenere che, **se l'ente *non profit*/associazione tratta i dati personali comuni e sensibili dei soci per gli scopi statutari e non li comunica a terzi e non li diffonde, non ha l'obbligo di acquisire il consenso/autorizzazione dei soci.**

Un profilo più delicato è quello di capire, ai fini dell'esonero dal consenso, quali siano le persone che hanno "contatti regolari con l'ente", ed in genere la posizione dei **beneficiari dell'attività**.

*Gli articoli 24 e 26, infatti, si riferiscono a quelle persone che fanno parte dell'organizzazione dell'ente (siano essi volontari/ associati o no), ma non sembrano riguardare i beneficiari dell'attività. In ogni caso, l'aver contatti regolari con il beneficiario (perché si fornisce a lui un servizio continuativo) comporta per l'ente non profit l'esonero dall'obbligo di richiedere il suo consenso solo in relazione ai **dati comuni**; quando si tratta di **dati sensibili** (es. sanitari), l'esonero sembra scattare, in base all'art. 26, solo per gli enti non profit "a carattere politico, filosofico religioso o sindacale", e quindi non riguarda la maggior parte degli enti non profit e delle Odv.*

Gli articoli 24 e 26 stabiliscono inoltre che le modalità di utilizzo dei dati vadano "previste espressamente con **determinazione resa nota agli interessati** all'atto dell'informativa ai sensi dell'art. 13".

*Si consiglia pertanto di stabilire le modalità dei trattamenti dei dati dei soci con una apposita **delibera del Consiglio Direttivo** (saranno sostanzialmente le stesse modalità da descrivere poi nel Documento Programmatico sulla Sicurezza), da citare poi nell'informativa.*

Con riferimento ai beneficiari e comunque ai non soci, possono però applicarsi alle associazioni anche altre ipotesi di esclusione:

> Il consenso al **trattamento dei dati comuni non è richiesto** quando il trattamento (art. 24):
> a) è necessario per adempiere ad un *obbligo previsto dalla legge*, da un regolamento o dalla normativa comunitaria;
> b) è necessario per eseguire *obblighi derivanti da un contratto* del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
> c) riguarda dati provenienti da *pubblici* registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità

che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
d) riguarda *dati relativi allo svolgimento di attività economiche*, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale

Il consenso al **trattamento dei dati sensibili non è richiesto** quando il trattamento (art. 26, comma 4 lett. a) è necessario "per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111" o quando il trattamento (art. 26, comma 4 lett. b) è necessario "per la salvaguardia della vita o dell'incolumità fisica di un terzo".

*Le norme di cui sopra consentono all'associazione/ente non profit di **non chiedere il consenso** se il trattamento:*

- *dei dati comuni e sensibili è necessario per l'adempimento degli obblighi nascenti dal **rapporto di lavoro** con i propri dipendenti;*
- *consiste nella comunicazione obbligatoria dei dati comuni all'Agenzia delle Entrate;*
- *consiste nella comunicazione dei dati comuni degli associati alla compagnia di assicurazione da parte delle Odv iscritte ai registri per l'**assicurazione obbligatoria di cui all'art. 4 L. 266/91**;*
- *dei dati comuni serve per eseguire un servizio richiesto dal beneficiario (es. richiesta di trasporto o assistenza domiciliare);*
- *di dati sensibili serve per la tutela della vita o incolumità fisica della persona [32].*

*Per quanto riguarda i cd. **DATI PUBBLICI** (cfr. art. 24, lett. c) occorre non fare confusione: sono pubblici i dati conoscibili da chiunque per espressa*

[32] In applicazione di questo principio, i volontari e gli enti che prestano servizio nell'ambito del Sistema di Urgenza ed Emergenza Medica (Suem) 1-1-8 non sono tenuti ad acquisire il consenso scritto del paziente/infortunato di cui acquisiscono i dati. Particolari semplificazioni sono previste anche per l'informativa o nei casi in cui il servizio si inserisce in un sistema di convenzionamento con il S.S.N.





*disposizione di **legge** [33]; per il resto la grande diffusione di alcuni dati non significa che siano liberamente utilizzabili per qualsiasi scopo[34].*

In definitiva, si consiglia:

→ **di chiedere il consenso scritto ai beneficiari dell'attività se si trattano loro dati sensibili**;

→ **chiedere il consenso orale o scritto ai beneficiari se si trattano loro dati comuni**

E va comunque tenuto presente:

→ che anche in caso di esonero dal consenso, **va sempre fornita all'interessato l'informativa**, nella quale descrivere specificamente le modalità con cui l'associazione utilizza i dati [35]

→ che **i dati sanitari**, ovvero quei dati idonei a rivelare lo stato di salute e la vita sessuale, **non possono essere diffusi, nemmeno su consenso dell'interessato**.

[33] Ad esempio non sono conoscibili da chiunque, ma solo dall'interessato, i *dati anagrafici*.
[34] Cfr. D/R n. 28.
[35] Cfr. D/R n. 9.

## 14. Come va richiesto il consenso per il trattamento dei dati "comuni" e "sensibili"?

L'art. 23 stabilisce le caratteristiche dell'autorizzazione/consenso:

> Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.
> Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.
> Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili

Secondo la legge quindi il consenso al trattamento dei dati deve essere:

- **espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto).
- **libero**, cioè manifestato liberamente dal soggetto, richiesto in termini non definitivi e non incondizionati[36]. Inoltre il consenso non può essere imposto, se invece è facoltativo[37].
- **specifico**, ovvero riferito ad uno o più trattamenti individuati e aventi specifiche finalità.
- **informato**, ovvero preceduto dall'informativa di cui all'art. 13.
- **documentato per iscritto** in caso di **dati comuni**.

Significa che l'associazione può anche ottenerlo **oralmente** (incerto se per via telefono) e contestualmente **annotare** di averlo ricevuto in un apposito registro (o nel libro soci) da conservare in sede.

Per maggiore sicurezza è consigliabile comunque ottenere una sottoscrizione dell'interessato, o comunque conservare prova dell'avvenuta autorizzazione.

[36] Ad esempio non si potrà chiedere il consenso per ogni trattamento futuro svolto con qualunque modalità.
[37] Ad esempio l'Odv non potrà imporre all'aderente di prestare il consenso al trattamento dei suoi dati per finalità estranee all'associazione, pena la sua mancata iscrizione.





Si possono a tal proposito utilizzare gli accorgimenti già individuati a proposito dell'informativa[38], anche perché la richiesta di consenso deve essere sempre preceduta/accompagnata dall'informativa.

*Quindi:*

- *per quanto riguarda i nuovi soci/aderenti**, l'informativa e la richiesta di consenso possono essere allegati o contenuti nella domanda di adesione all'associazione**, o scritti nel retro[39].*
- *la richiesta di consenso per il trattamento di dati "comuni" può essere anche spedita **via fax o via mail**. Nel primo caso, però, potrebbe non ritenersi sufficiente per l'associazione conservare la ricevuta di avvenuto invio: un consenso espresso si può infatti configurare solo se l'interessato rispedisce il fax firmato (o lo faccia pervenire firmato in associazione). Se la richiesta di consenso è inoltrata via e-mail potrebbe forse bastare un e-mail di "conferma" (che l'ente potrà stampare e conservare) da parte dell'interessato, quando però gli sia stato reso chiaramente noto che il messaggio di risposta sarà inteso quale autorizzazione al trattamento.*
- *se l'associazione gestisce un sito web esiste la possibilità di utilizzare il cd. **point&click**, ovvero di creare attraverso appositi software una pagina web nella quale l'interessato può accedere (anche utilizzando una password appositamente comunicata dal titolare), per fornire i propri dati personali, per essere informato delle modalità del trattamento, e soprattutto per autorizzare il trattamento barrando una o più caselle; successivamente, anche per modificare o revocare la propria autorizzazione ed esercitare i diritti di cui all'art. 7. Tale operazione rende molto semplice per le associazioni la raccolta dei dati, la comunicazione dell'informativa e l'acquisizione del consenso e si traduce in un buon risparmio di tempo per chi richiede e fornisce il consenso; importa però una certa spesa e l'intervento di un tecnico esperto, poiché richiede il rispetto di alcuni precisi requisiti di sicurezza e riservatezza delle transazioni informatiche, da valutare a seconda della tipologia dei dati forniti. E' pertanto consigliata solo per le grandi associazioni.*
- *il consenso va acquisito **una sola volta** se il trattamento dei dati non cambia e rispetta le finalità indicate nell'informativa medesima;*
- *il consenso va richiesto **solo a quei soggetti dei quali l'associazione raccoglie, registra o utilizza i dati**, e tra costoro non rientrano ovviamente i soggetti beneficiari dell'attività istituzionale che l'ente non identifica.*

[38] Cfr. D/R n. 9.
[39] Come visto sopra, nel caso di soci/aderenti il consenso non è necessario, salvo però che non si comunichino i dati a terzi o non si diffondano e siano comunque rispettate le condizioni dell'art. 24, comma 1 lett. e), a meno che non si rientri in altre ipotesi di esclusione del consenso.

- *se l'associazione ha chiesto e ottenuto il consenso nel vigore della vecchia legge (la L. n. 675/96) non avrà l'obbligo di acquisirlo nuovamente, a meno che i trattamenti che svolge si siano a tal punto modificati da richiedere un'autonoma manifestazione di volontà dell'interessato.*

  La richiesta di autorizzazione/consenso, che si propone in **modello**, va quindi trasmessa personalmente all'interessato e deve essere preceduta dall'informativa di cui all'art. 13 del Codice.

  *Come è ovvio, l'acquisizione del consenso è abbastanza facile se l'interessato è un socio o un collaboratore dell'associazione; se invece è un* ***beneficiario*** *(si pensi ad esempio ad una persona anziana) potrebbero sorgere problemi e comunque un adempimento burocratico poco si adatta alla situazione. Certo che, se si ritiene necessario il consenso (perché il trattamento non rientra nelle ipotesi di esclusione o perché si ritiene comunque di acquisirlo), il mezzo più sicuro, anche i relazione ai dati comuni, è la sottoscrizione dell'interessato, perché consente al Titolare di dimostrare di averlo ricevuto.*

  Nonostante il silenzio del Codice, si deve ritenere che, se l'interessato è minorenne il consenso vada prestato da chi ha la rappresentanza legale, e cioè i genitori che hanno la potestà o il tutore se esiste[40].

  **ATTENZIONE**: **in caso di DATI SENSIBILI, il consenso deve essere SCRITTO, e quindi la sottoscrizione dell'interessato è obbligatoria**.

  La richiesta di autorizzazione/consenso va quindi fatta sottoscrivere personalmente all'interessato e deve essere preceduta dall'informativa di cui all'art. 13 del Codice. In tal caso, invece di firmare per "presa visione" dell'informativa, l'interessato firmerà per autorizzazione/consenso al trattamento[41].

  *Come visto, non è semplice districarsi tra norme, ipotesi di esclusione, o capire se si sta svolgendo un trattamento di dati sensibili, o se effettivamente si pone in essere una comunicazione o una diffusione di dati e via dicendo. Gli esempi e le D/R di cui sopra dovrebbero fornire un valido aiuto; nel dubbio è forse preferibile, in caso di incertezza, far sottoscrivere il consenso, sia per i dati*

[40] Si tenga presente che il Garante ha più volte precisato, nel caso di diffusione di notizie relative a minori con il mezzo televisivo, che il consenso dei genitori può alle volte non essere sufficiente, se il trattamento lede comunque la riservatezza del figlio (cfr., ad esempio, Provv. 15.11.2001 e Comunicato Stampa 11.12.2002 in **www.garanteprivacy.it** o **www.garanteprivacy.it**).

[41] Informativa e richiesta di consenso possono/debbono essere contenute nella stessa pagina, unendo i modelli I, II o III (togliendo la firma del titolare e dell'interessato per "presa visione") con i modelli V o VI.





*comuni che per i dati sensibili, soprattutto nei casi in cui l'associazione ha "fisicamente" la possibilità di far sottoscrivere l'interessato.*

## 15. Le associazioni devono chiedere l'autorizzazione al Garante per il trattamento dei dati sensibili e sanitari?

Il Codice all'art. 26 dice che i dati sensibili possono essere trattati solo previa autorizzazione del Garante.

Tuttavia gli enti non profit non devono chiedere tale autorizzazione, avendo il Garante provveduto, ai sensi dell'art. 40 del Codice, a rilasciare due autorizzazioni generali, cui attenersi:

a) **AUTORIZZAZIONE n. 3 del 28.6.2007** 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;

b) **AUTORIZZAZIONE n. 2 del 28.6.2007** per il trattamento dei dati idonei a rivelare lo stato di salute e al vita sessuale.

Tali autorizzazioni (efficaci sino al 30 giugno 2008) "coprono" il trattamento svolto dai soggetti non profit (associazioni, organizzazioni assistenziali o di volontariato, ONLUS, Cooperative sociali, fondazioni) dei dati sensibili di aderenti, aspiranti soci, beneficiari dell'attività e in genere soggetti che hanno contatti stabili con l'associazione, raccolti presso questi soggetti, quando il trattamento è svolto per il perseguimento degli scopi istituzionali nonché il trattamento di dati sanitari svolto da "organizzazioni di volontariato o assistenziali, limitatamente ai dati e alle operazioni indispensabili per perseguire scopi determinati e legittimi previsti, in particolare, nelle rispettive norme statutarie".

Resta fermo l'obbligo di acquisire il **consenso scritto** dell'interessato nei casi in cui è necessario[42].

*L'autorizzazione n. 3/07 è riportata negli allegati; le altre autorizzazioni si possono trovare nel sito www.privacy.it nel link "Garante – Autorizzazioni" e www.garanteprivacy.it.*

[42] Cfr. D/R n. 13.





## 16. Cosa sono i dati giudiziari?

I dati giudiziari sono i "dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (art. 4, comma 1, lett. e)

*Sono quindi dati giudiziari molte delle annotazioni (di natura penale) che risultano dal **Casellario Giudiziale**, tra cui le sentenze di condanna e i decreti penali irrevocabili, le misure di sicurezza poste a carico di un individuo, i provvedimenti di amnistia e altri. Non invece le sentenze e i provvedimenti civili. Possono entrare a contatto con dati giudiziari le associazioni che operano nella realtà carceraria o che raccolgono ex-carcerati (al pari delle cooperative sociali) nell'ipotesi in cui in qualche modo utilizzino o conservino dati relativi al passato o presente giudiziario degli aderenti o dei beneficiari.*

In base all'art. 27, "il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili".

Il Garante ha regolato il trattamento di dati giudiziari con l'**AUTORIZZAZIONE GENERALE n. 7** del 28.6.2007 (*nel sito www.privacy.it nel link "Garante" – "Autorizzazioni o in www.garanteprivacy.it.*) che consente il trattamento di dati giudiziari dei soci e dei beneficiari anche ad associazioni anche non riconosciute, a scopo assistenziale o di volontariato, a fondazioni, comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, nonché a cooperative sociali e società di mutuo soccorso, ad enti e associazioni che curano il patrocinio, il recupero, l'istruzione, la formazione professionale, l'assistenza socio-sanitaria, la beneficenza e la tutela di diritti in favore dei soggetti cui si riferiscono i dati o dei relativi familiari e conviventi, quanto il trattamento è indispensabile per perseguire scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo.

Per il trattamento dei dati giudiziari non è prevista alcuna acquisizione del consenso dell'interessato.

## 17. Cosa sono le misure di sicurezza?

Sono accorgimenti, procedure e strumenti di custodia e controllo informatico e non informatico dei dati che hanno lo scopo di "ridurre al minimo i rischi di distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta" (art. 31).

Di fondamentale importanza è la distinzione tra misure di sicurezza minime e misure di sicurezza idonee.

a) Le **MISURE MINIME** sono quelle che il Codice e il **disciplinare tecnico** allegato al Codice (in seguito anche D.T.[43]) indicano come necessarie ad assicurare un livello minimo di protezione, e variano a seconda che il trattamento di dati sia svolto
   - **con strumenti elettronici** (art. 34 del Codice e nn. 1-18 del D.T.)
   - **senza strumenti elettronici** (art. 35 del Codice e nn. 27-29 del D.T.)
   - **riguardi dati sensibili** (nn. 19-24 del D.T.)

Alcune misure erano già previste e andavano quindi adottate – anche se con modalità ed in casi parzialmente differenti da quelli previsti dal Codice – in base alla disciplina precedente (D.P.R. 318/99). La distinzione tra misure "vecchie" e "nuove" (previste per la prima volta nel Codice) non è però facile e netta. Il D.P.R. 318/99 già prevedeva, ad esempio, l'attribuzione di parole chiave agli incaricati, l'installazione di antivirus, il Documento Programmatico sulla Sicurezza[44].

[43] Il Disciplinare Tecnico allegato al Codice (e riportato anche qui tra gli allegati) non ha valore di legge, ma di regolamento; non è soggetto all'approvazione del Parlamento, ma è emesso con decreto del Presidente della Repubblica su proposta del Ministro di grazia e giustizia, sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante. La ragione sta nel fatto che le misure minime variano a seconda dell'evoluzione tecnologica, e lo strumento del regolamento consente un aggiornamento molto più rapido della disciplina.

[44] Il DPS era però richiesto solo nel caso che il trattamento si svolgesse con computer "accessibili alla rete mediante una rete di telecomunicazioni disponibili al pubblico".





*Le misure minime "nuove" dovevano essere adottate entro il **31 marzo 2006**, o, in casi particolari, entro il **30 giugno 2006** [45]: sono quindi al momento tutte obbligatorie.*

La mancata adozione è colpita dalla sanzione penale dell'arresto sino a due anni o dell'ammenda da € 10.000 a € 50.000.

*L'adozione delle misure di sicurezza è uno dei punti più delicati della disciplina, anche perché i profili giuridici si intersecano con nozioni e strumenti tecnici.*

b) Le **MISURE DI SICUREZZA IDONEE** sono invece tutte quelle che, ulteriori e "migliori" rispetto alle minime perché corrispondenti allo stato della tecnica, sono comunque da adottarsi per ridurre al minimo i rischi del trattamento, e la cui mancata adozione comporta l'esposizione del titolare al rischio di dover risarcire in sede civile i danni subiti da terzi[46] per effetto della distruzione e perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

Per quanto riguarda **le associazioni, è importante che esse adottino in primo luogo le misure minime**, per liberarsi da eventuale responsabilità penale, secondo le indicazioni delle D/R successive. L'adozione di ulteriori misure andrà valutata invece in base ad ogni singola realtà associativa, alle dimensioni dell'associazione, ai tipi di trattamenti che vengono svolti, al grado di rischio che subiscono i dati personali trattati.

[45] L'art. 180 del Codice come modificato da ultimo dal decreto cd. *milleproroghe* (decreto legge n. 273/05) convertito in legge n. 51 del 23.2.2006, consentiva di prorogare la data del 31 marzo 2006 fino al **30 giugno 2006** a quei titolari che disponevano di strumenti elettronici i quali per obiettive ragioni tecniche non consentivano in tutto o in parte l'immediata applicazione delle misure minime. Tali soggetti dovevano descrivere tali ragioni tecniche in un documento/lettera avente data certa da conservare presso la propria struttura (sede), e nel frattempo adottare ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31. **Non essendoci state altre proroghe, il termine del 30 giugno 2006 deve considerarsi termine ultimo per l'adozione delle misure di sicurezza**.

[46] Cfr. D/R n. 25.

## 18. Quali misure di sicurezza minime sono richieste in caso di trattamento dei dati con strumenti elettronici?

L'adozione delle misure di sicurezza minime in caso di trattamento dei dati mediante computer è uno degli obblighi cui i titolari devono prestare più attenzione.

Vi sono soggette tutte le associazioni che, per la gestione dell'attività istituzionale, contabile o amministrativa (anche solo per raccogliere i dati dei propri aderenti e gestire la corrispondenza) utilizzano **anche un solo computer, anche se privo di connessione ad internet**.

Le misure minime di sicurezza sono:
- un sistema di autenticazione informatica
- un sistema di autorizzazione
- un sistema di protezione del computer da virus e accessi indesiderati[47]
- un sistema di conservazione dei dati attraverso copie di sicurezza
- il documento programmatico sulla sicurezza

***Le prescrizioni del Codice e del Disciplinare Tecnico riguardano tutti i soggetti che trattano dati mediante computer**, dall'impresa multinazionale, alla clinica privata, allo studio professionale di grandi dimensioni, fino ad arrivare agli enti non-profit, alle associazioni non riconosciute di medie e piccole dimensioni, addirittura alle persone fisiche. Tuttavia probabilmente il livello di complessità e di raffinatezza delle protezioni va parametrato alle **dimensioni** del soggetto/ente e al **grado di rischio** che i dati trattati subiscano perdite, intrusioni, alterazioni e dispersioni non consentite.*

*Quindi, ad esempio, enti di ridotte dimensioni che trattano unicamente nell'unico computer presente in sede (o di proprietà del Presidente o di un consigliere) i dati relativi ai nominativi, agli indirizzi e alle informazioni anagrafiche degli associati, assolveranno il loro compito adottando quelle misure elementari (password, antivirus aggiornato semestralmente e altri accorgimenti) idonee e sufficienti in ragione della particolare situazione.*

*D'altra parte, bisogna tener presente:*
- *che **non vi sono deroghe esplicite** per enti di modeste dimensioni o realtà che raccolgono dati per fini di volontariato o comunque per fini ideali;*
- *che le norme in tema di privacy rappresentano comunque una forma di tutela per le associazioni stesse e un **miglior servizio** reso ai propri aderenti, ai beneficiari dell'attività istituzionale e alla collettività in genere;*

[47] Misura già parzialmente obbligatoria in base alla disciplina precedente.





- *che la tutela dei dati personali si rivela ancor più necessaria con riferimento a quelle associazioni, molte nel Veneto, che operano in **settori delicati** (sanità, disabilità, disagio sociale) utilizzando quindi un gran numero di dati cd. "sensibili", e magari gestendoli mediante computer in rete tra loro e collegati ad internet molte ore al giorno o in via stabile (ADSL), e dunque con rischi alti di intrusione o perdita. Tali associazioni dovranno probabilmente dotarsi di sistemi di sicurezza (antivirus, firewalls, routers, meccanismi di back up, ecc.) al pari di ogni analoga realtà aziendale.*

Per un quadro delle misure di sicurezza da adottare in rapporto al sistema informatico dell'associazione, cfr. le **D/R seguenti** e la "**scheda tecnica**".

## 19. Che cos'è un sistema di autenticazione informatica?

Consiste essenzialmente nell'attribuzione al soggetto o ai soggetti che all'interno dell'associazione gestiscono i dati mediante computer (Incaricati) delle cd. *credenziali di autenticazione*, ovvero di un codice o di un dispositivo di identificazione personale o **USER-NAME** e di una parola chiave o **PASSWORD**, in modo che solo questi soggetti e non altri estranei possano accedere ai computer e gestire i dati secondo i loro compiti e l'ambito a loro attribuito.

I codici di identificazione più semplici sono quelli basati sul sistema *username* e *password*; i più sicuri sono invece quelli che sfruttano le caratteristiche biomediche (voce o impronta del pollice). Chiaramente la prima soluzione è quella meno dispendiosa.

L'*username* non può essere assegnato a diversi incaricati, nemmeno in tempi differenti.

*Quanto alle password, generalmente sono determinate pensando alla data di nascita, ai familiari, a parole di senso comune. Tuttavia queste password non sono sicure, perché facilmente decifrabili.*

Per questo il Disciplinare Tecnico prevede che la password:
- deve essere di almeno 8 caratteri oppure dal numero massimo di caratteri consentito dallo strumento elettronico, e non deve contenere elementi facilmente ricollegabili alla persona del suo utilizzatore/incaricato
- deve essere conosciuta solamente dall'incaricato e quindi memorizzata dall'incaricato/utilizzatore del computer o conservata in modo da impedire la conoscenza di estranei *(es. busta chiusa in un cassetto chiuso, oppure conservata da una sola persona[48] con opportune cautele)*
- è personale e non può essere assegnata a più incaricati *(non sono quindi ammesse password di gruppo)*
- deve essere sostituita/modificata dall'incaricato al primo utilizzo [*nei sistemi informatici complessi*] e, successivamente, almeno ogni sei mesi (tre mesi se si trattano dati sensibili o giudiziari)

[48] Potrà essere la persona nominata Responsabile, o anche l'Amministratore di sistema, o un altro degli incaricati in qualità di **"custode" delle password**.





*Come si può notare il D.T. vieta solamente di determinare la password usando elementi facilmente ricollegabili alla persona del suo utilizzatore, come il nome, il numero di C.F. e via dicendo. Si deve quindi ritenere che le misure minime di sicurezza siano rispettate anche se si utilizza per la password una parola di senso comune. Questa regola però non elimina completamente i rischi poiché ci sono, per esempio, programmi che in pochi minuti inseriscono automaticamente come password tutte le parole del vocabolario. Per questo* ***le password più efficaci sono quelle composte da numeri e lettere insieme*** [49]*: l'adozione di una password così formata configura probabilmente "misura idonea" ai sensi del Codice* [50]*.*

L'individuazione iniziale delle password e degli *username* è generalmente svolta da un soggetto esterno detto **AMMINISTRATORE DI SISTEMA**.

*Questa figura era stata prevista dal DPR 318/99, ma non è stata più riproposta nel Codice come figura giuridica. Ciò non toglie che, nei fatti, ci possa essere: si tratta appunto del tecnico o della ditta che adatta il sistema informatico alle esigenze del Titolare, impostando i sistemi di autenticazione e autorizzazione. Chiaramente se all'interno dell'associazione esistono le competenze tecniche per predisporre queste misure minime, l'intervento di un esterno non sarà necessario e amministratore di sistema sarà colui (dipendente, volontario, anche la stessa persona che è nominata Responsabile…) che se ne occupa.*

Le modifiche successive della password spettano invece in teoria al solo Incaricato; per favorire tale operazione i computer possono generalmente essere impostati in modo tale che richiedano periodicamente al proprio utilizzatore di cambiare la password.

Infine, il D.T. prevede che le credenziali di autenticazione vadano **disattivate** quando il suo utilizzatore cessa dalla qualità di incaricato (es. ex dipendente o ex socio) o quando non sono più utilizzate per più di sei mesi (es. maternità o malattia di una dipendente, infortunio).

[49] E' stato calcolato che se si utilizzano 8 caratteri alfanumerici un computer di media potenza impiegherebbe cinque anni a inserire tutte le combinazioni possibili.
[50] Cfr. D/R n. 17, lett. b.

## 20. Che cos'è un sistema di autorizzazione informatica?

Si ha quando il sistema informatico predisposto dal Titolare **distingue due o più "profili", ovvero due o più ambiti diversi in cui si svolgono i trattamenti elettronici di dati** all'interno dell'associazione, qualora il Titolare decida che uno o alcuni Incaricati possano svolgere solo determinati trattamenti e quindi possano accedere solo ad alcuni ambiti o programmi o banche dati, secondo il proprio "profilo". I profili possono riguardare "ciascun incaricato" ma anche "classi omogenee di incaricati", e devono essere individuati prima del trattamento (n. 13 del D.T.).

*Un esempio può chiarire meglio: una associazione può decidere che il semplice aderente/volontario non possa accedere ai computer, o possa utilizzare solo alcuni programmi (windows, ad esempio) senza avere accesso informatico a tutti i dati dell'associazione, ai rendiconti, ai verbali ecc., o che gli eventuali dipendenti accedano a banche dati diverse o tra loro o rispetto al Presidente o ai membri del Consiglio. Si tratta di operazioni che richiedono una certa esperienza nel settore informatico e quindi l'intervento di un tecnico (il cd. amministratore di sistema [51]).*

*Solo nei sistemi operativi più recenti o comunque dedicati all'uso professionale WINDOWS NT, WINDOWS 2000, WINDOWS XP, WINDOWS VISTA, MAC OS e LINUX (solo per indicarne alcuni) è possibile dividere in "pezzi" il sistema e far accedere a certi soggetti solo alcuni programmi e/o banche dati, a seconda dell'USER-NAME e della PASSWORD con cui entrano nel computer. Se si utilizzano altri sistemi operativi questa funzione deve essere gestita da un server (da un computer "centrale"), nel quale devono essere salvati tutti i dati.*

Per un quadro delle misure di sicurezza da adottare in rapporto al sistema informatico dell'associazione, cfr. anche la "**scheda tecnica**".

La predisposizione di un sistema di autorizzazione è necessaria solo se ci sono più "profili": **il titolare infatti può anche decidere che tutti gli incaricati accedano a tutti gli ambiti del trattamento che si svolge nella sua struttura** (cioè a tutte le banche dati o a tutti i programmi): in questo caso non sarà necessario un "sistema" perché il profilo di autorizzazione sarà unico (uno stesso profilo per tutti gli incaricati).

[51] Cfr. D/R n. 19.





In presenza di un unico profilo, l'eventuale "sbarramento" potrà essere posto a monte: **il titolare potrà cioè decidere di far accedere ai computer solo una ristretta cerchia di persone**, le sole cui saranno assegnate le credenziali di autenticazione (*Username* e *password*) necessarie ad usare i computer. Queste persone avranno tutte lo stesso "profilo", e potranno accedere all'intero sistema.

*Ci si chiede: può l'associazione decidere che, per comodità, la password sia una sola e, se pur attribuita formalmente ad una sola persona/incaricato, venga conosciuta e utilizzata per l'accesso al/ai computer da tutte le persone dell'associazione che abitualmente li usano?*

Questo in teoria non sarebbe consentito: a prescindere dall'attribuzione dello stesso profilo a "classi omogenee" di incaricati (es. volontari, membri del Consiglio, dipendenti addetti all'amministrazione), **il Codice richiede che a ciascun incaricato siano attribuite autonome e diverse credenziali di autenticazione, cioè un diverso USERNAME e una PASSWORD, per il solo fatto di svolgere un trattamento mediante computer**.

*Nel caso vi siano più profili di autorizzazione, la situazione sarà quindi la seguente: se il sistema elettronico è una casa, l'incaricato sarà un visitatore che userà le sue credenziali come una chiave che apre solo alcune porte o tutte le porte. Potrà pertanto accedere ad una sola, a varie o a tutte le stanze a seconda di quello che ha deciso per lui il "padrone di casa" consegnando a lui la chiave; nelle varie stanze potrà essere da solo (se non esistono altre chiavi oltre alla sua che consentono ad altri visitatori di entrare in quella stanza) o trovare altre persone che vi sono entrate con la loro chiave personale, diversa dalla sua e da quella di ciascun altro ma idonea ad aprire quella stessa serratura (ed eventualmente anche altre).*

I profili di autorizzazione e il sistema di autenticazione vanno verificati almeno una volta all'anno (n. 14 del D.T.).

## 21. L'associazione deve nominare i propri incaricati al trattamento?

**SI**, la designazione degli incaricati è un obbligo regolato dall'art. 30 del Codice:

> 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 è effettuata **per iscritto** e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

La nomina degli incaricati, con le opportune istruzioni, è **necessaria anche se l'incaricato esegue solo trattamenti "cartacei" e non informatici**. Quando l'incaricato utilizza il computer, la sua designazione e la delimitazione del suo trattamento rientra nel cd. sistema di autorizzazione e costituisce misura di sicurezza "minima"[52].

Il titolare potrà consegnare all'incaricato una **lettera di incarico**[53] nella quale lo designa come tale, indica che trattamenti egli può svolgere, su che dati, con quali modalità e nel rispetto di quali misure di sicurezza. Se l'incaricato svolge un trattamento informatico i "confini" del saranno corrispondenti al "profilo di autorizzazione"[54]. Chiaramente se i profili sono uguali le lettere di incarico potranno avere lo stesso identico contenuto anche se consegnate a diversi incaricati.

*In alternativa, l'art. 30 ritiene sia sufficiente la "preposizione scritta dell'incaricato ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima": questa opzione, si capisce, riguarda gli ambiti aziendali, ed è forse poco adattabile alla realtà delle associazioni non profit.*

Più importante sembra la **lista degli incaricati**[55] con i relativi profili di autorizzazione, che il titolare (n. 15 del D.T.) deve scrivere e aggiornare periodicamente almeno una volta all'anno: tale lista può

[52] Cfr. D/R n. 17 e 20.
[53] Cfr. modello/esempio VII (nomina ad incaricato del trattamento).
[54] Cfr. D/R n. 20.
[55] Cfr. modello/esempio XII (lista degli incaricati e manutentori).





essere o **nominativa** o individuare **classi omogenee** (es. volontari/aderenti, dipendenti, membri del Consiglio, ecc.), e deve anche contenere i nominativi degli addetti alla gestione e manutenzione degli strumenti elettronici (compreso quello precedentemente detto "amministratore di sistema")

Infine, è fatto obbligo ad ogni titolare di assicurare la **formazione degli Incaricati** attraverso[56]:

> interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali

[56] Cfr. punto 19.6 del Disciplinare Tecnico allegato al Codice sul contenuto del DPS (D/R n. 23).

## 22. Che cos'è un sistema di protezione informatica?

Un sistema di protezione del computer serve ad evitare o limitare l'attacco di virus o le intrusioni indesiderate ed in genere l'attacco di "programmi pericolosi"[57].

*Programmi pericolosi sono quelli (virus, worm, malware, ecc.), che danneggiano file, programmi e sistemi, o si installano nel computer per compiere operazioni all'insaputa dell'utilizzatore (ad esempio attivano automaticamente la connessione ad internet). I virus "attaccano" automaticamente anche solo sulla base dell'accesso a internet o alla posta elettronica o della "visita" ad un determinato sito. Una condotta sicura sarebbe quella di non inserire e non trattate i dati personali dell'associazione nel computer con cui si naviga in rete, in modo da evitare "contaminazioni" indesiderate. Tale scelta è un rimedio forse un po' troppo drastico e comunque dispendioso, considerato che le associazioni hanno spesso un solo computer con cui gestiscono insieme le banche dati e accedono a internet e alla posta elettronica.*

Se quindi il computer o la "rete" di computer dall'associazione viene collegata a internet o ha un programma di posta elettronica e contiene altresì dati personali (e magari anche sensibili), le misure da adottare dovranno essere più incisive.

Il Codice e soprattutto il Disciplinare Tecnico richiedono:

→ l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale per evitare l'intrusione, l'azione di programmi pericolosi e l'accesso abusivo al computer

Per evitare l'azione dei programmi pericolosi lo strumento assolutamente **obbligatorio** e più idoneo è un **valido e aggiornato ANTIVIRUS.**

*Il Codice ne prescrive un aggiornamento semestrale, ma se si accede a internet l'aggiornamento andrebbe fatto molto più spesso, addirittura settimanalmente (esiste la possibilità di aggiornarlo automaticamente dalla rete).*

Contro l'intrusione indesiderata lo strumento migliore è il cd. **FIREWALL** (in inglese "porta antifuoco"), che consente di bloccare le intrusioni dall'esterno da parte di hacker o di software dannosi che

[57] Ovvero quelli di cui all'art. 615 *quinquies* del codice penale.



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

utilizzano accessi particolari per recare danno ai computer. Ne esistono in versione hardware e software (più economica e già inclusa in alcuni sistemi operativi come WINDOWS XP e LINUX), utilizzabili nello stesso momento da più computer in rete tra loro.

*Il firewall ha un certo costo e come detto è uno strumento dall'utilità abbastanza limitata, perché evita l'accesso ai computer ma non protegge dai pericoli più concreti, e cioè i virus; tuttavia costituisce uno strumento consigliato per chi utilizza il computer con costanza e con frequente (o permanente tramite ADSL) accesso ad internet. Infine, esistono anche alcuni "combinati" cioè firewall che contengono antivirus potenti che si aggiornano in automatico rendendo l'utente libero di navigare senza doversi preoccupare di alcunché. Per un quadro delle misure di sicurezza consigliabili in rapporto al sistema informatico dell'associazione, cfr. anche la "scheda tecnica".*

→ L'**aggiornamento periodico** (ogni anno e ogni sei mesi in caso di trattamento di dati sensibili) dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti

*Si tratta di una misura di sicurezza introdotta per la prima volta con il Codice. Questo aggiornamento periodico riguarda i programmi e i sistemi operativi installati nel computer (office, windows ecc.) ed è costituito da versioni successive o migliorative (i cd. **patch**) dei programmi medesimi che ne eliminano gli errori o le falle, in modo da limitarne la vulnerabilità da parte di estranei. Vi è da dire che l'aggiornamento mediante patch di sicurezza non è priva di rischi: essi infatti alle volte eliminano certe falle ma ne creano altre. Senza contare che le case produttrici, quando il sistema operativo è ormai superato, eliminano la produzione del relativo patch: in questo caso sarebbe opportuno cambiare il sistema operativo.*

→ Il **salvataggio** dei dati con frequenza almeno settimanale su supporti rimovibili che vanno opportunamente custoditi

Tale salvataggio consiste nella predisposizione di **COPIE DI SICUREZZA** o di **BACK-UP**, e cioè nella memorizzazione in dischetti o supporti esterni e rimovibili (nastri, dischetti, cd-rom).

*Tali supporti devono essere conservati in un luogo diverso da quello dove si trovano i computer che contengono i dati originali (per evitare, ad esempio, che un incendio possa distruggere entrambi). Si consiglia almeno di formare delle copie di back-up contenenti le banche dati (es. dei soci) e i documenti principali (es. verbali di assemblea).*

L'adozione delle misure sopra descritte (antivirus, firewall, aggiornamenti dei sistemi…) richiede, se non si è esperti di computer, l'assistenza di un tecnico. Potrà essere lo stesso soggetto nominato **AMMINISTRATORE DI SISTEMA**. Se ci si avvale di un soggetto esterno il D.T. dice che:

Il titolare riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico (punto 25 D.T.)

Il tecnico sarà tenuto quindi a rilasciare una specifica **attestazione/certificato di conformità**, nel quale egli dichiari di aver dotato il computer o i computer di determinate protezioni e che tali strumenti sono conformi a quanto richiesto dal nuovo Codice in tema di misure di sicurezza.

*La portata di tale certificato non è per la verità individuata dal Codice o dal D.T., e sono incerte le responsabilità che si assume colui che lo rilascia. Certamente sarà interesse del "tecnico" l'adozione di misure di sicurezza più sicure (e costose), al fine di evitare future responsabilità; l'associazione avrà invece l'esigenza di adottare le misure appena sufficienti per ritenersi "in regola". Per un quadro delle misure di sicurezza da adottare in rapporto al sistema informatico dell'associazione, cfr. anche la "**scheda tecnica**". In ogni caso l'attestazione non libera il titolare dall'onere di mantenere le misure minime adeguate (ad esempio aggiornare l'antivirus), e il tecnico, naturalmente, non sarà responsabile per modifiche svolte dall'utilizzatore che hanno eliminato le protezioni installate, o se il titolare, dopo l'intervento, decide di svolgere dei trattamenti di dati che richiedono misure più sicure. In generale è consigliato rivolgersi ad un **tecnico di fiducia**, con cui iniziare un rapporto di collaborazione, e che curi non solo l'installazione ma anche la manutenzione dei sistemi operativi ed elettronici.*

*La difesa da programmi pericolosi e virus si attua anche attraverso altri **accorgimenti e attenzioni** da parte dell'incaricato/utilizzatore del computer, non obbligatorie ma consigliabili, come ad esempio:*

- *non aprire e-mail o allegati dall'incerta o pericolosa provenienza;*
- *ridurre al minimo le operazioni di "sharing", e cioè di condivisione di file con altri connessi ad internet (con programmi come ad es. Kazaa, VinMX, Emule, ecc.) utilizzando opportuni accorgimenti e limitando la condivisione delle proprie risorse;*
- *non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;*





- *tenere sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti/programmi; disattivare sul browser l'esecuzione automatica degli script Java e Activex;*
- *ridurre al minimo l'invio di posta elettronica in formato "htlm";*
- *eseguire periodicamente la pulizia del disco fisso da "cookies", file temporanei ecc.;*
- *evitare i falsi allarmi e le catene di sant'Antonio, controllando preventivamente la bontà delle informazioni prima di diffonderle (ad esempio grazie a siti specializzati come www.attivissimo.info/antibufala/elenco.htm).*

*Nel 90% dei casi l'utilizzo di queste attenzioni, unite alla diligenza nel tenere aggiornato l'antivirus è assolutamente sufficiente. Una volta individuato il tecnico di fiducia, si consiglia, più che dotarsi di strumenti particolari e particolarmente costosi, di stabilire con lui un accordo di assistenza annuale che preveda alcune visite di controllo per verificare le procedure attuate dagli operatori, evitando così "falle" sulla sicurezza.*

Il D.T. prevede inoltre che il titolare debba impartire agli incaricati istruzioni per:

→ **non lasciare incustodito e accessibile il computer** durante una sessione di trattamento.

Le istruzioni saranno contenute nella **lettera di incarico**[58] e potranno comprendere, oltre al sistema delle "credenziali di autenticazione", e un semplice e tradizionale controllo visivo, anche uno *screensaver* abbastanza frequente e coperto da password.

Particolari e ulteriori regole sono dettate dal D.T. in caso di trattamento mediante computer di **dati sensibili o giudiziari**:

→ predisporre un sistema di conservazione dei dati e dei sistemi attraverso **copie di sicurezza**, per consentirne il ripristino in caso di perdita o distruzione in tempi certi compatibili con i diritti dell'interessato ed in ogni caso non superiori a sette giorni
→ **distruggere i supporti esterni** quando non sono più utilizzati o cancellarne definitivamente il contenuto quando sono utilizzati da altri incaricati[59].

[58] Cfr. modello/esempio VII.
[59] Si ricordi che la semplice cancellazione dei file dai dischetti non comporta la loro distruzione/eliminazione definitiva; è necessaria una completa formattazione.

## 23. Che cos'è il Documento Programmatico sulla Sicurezza (D.P.S.)? Quando va aggiornato?

Il DPS è un documento in carta semplice che deve essere redatto **da coloro che trattano dati sensibili o giudiziari con strumenti elettronici**. Secondo l'opinione prevalente vi sono tenuti in generale **tutti coloro che svolgono un trattamento informatico**, qualunque sia la tipologia di dati[60].

**Si consiglia quindi a tutte le Odv che svolgono un trattamento elettronico di scrivere un DPS, anche semplice**, considerata anche la buona probabilità che all'interno dell'associazione si trattino dati sensibili.

Nel DPS si devono descrivere sinteticamente tutti gli accorgimenti e le misure di sicurezza adottate e che si adotteranno, in base al Codice, per evitare il più possibile e comunque ridurre i rischi derivanti dal trattamento dei dati personali. Il suo contenuto è indicato dall'art. 34 del Codice e soprattutto nel punto 19 del D.T. Si tratta di un compito importante anche per le associazioni, considerato anche che la mancata predisposizione del DPS costituisce contravvenzione (cfr. art. 169 del Codice), ed ha come pena l'arresto sino a 2 anni o l'ammenda da 10.000 a 50.000 euro[61].

Il DPS non deve essere comunicato a terzi ma **conservato presso la sede** dell'associazione.

Incertezza è sorta in ordine al problema di **quando il DPS vada aggiornato.**

Il D.T. dice che il DPS va redatto "**entro il 31 marzo di ogni anno**" e che l'aggiornamento periodico della lista degli Incaricati deve avere cadenza "almeno annuale".

[60] Questa interpretazione è fondata sulla circostanza per cui il Codice, che ha valore di legge, all'art. 34 lett. g) impone il DPS quale misura minima di sicurezza nel caso di trattamento di dati con strumenti elettronici, ed è solo il Disciplinare Tecnico (che non ha valore di legge, ma di regolamento), a specificare che il DPS va redatto dai titolari "di un trattamento di dati sensibili o di dati giudiziari" (cfr. punto n. 19.1 del D.T.).
[61] Cfr. D/R n. 25.





L'art. 34 del Codice impone invece la tenuta di un "aggiornato Documento Programmatico sulla Sicurezza", sanzionata addirittura penalmente.

*In base alla norme di cui sopra si può dire che **le associazioni possono limitarsi ad aggiornare il DPS una volta all'anno, entro il 31 marzo**. Se in altre parti dell'anno apportassero alle misure di sicurezza delle modifiche rilevanti (es. cambio di tutti i computer), potrebbe essere opportuno modificare il DPS in occasione di quella variazione.*

*Probabilmente da escludere è la necessità che il DPS o il suo aggiornamento abbiano **data certa**, e cioè sia possibile risalire con certezza (giuridica) al giorno in cui è stato redatto o aggiornato (ad esempio attraverso l' "autospedizione" presso gli uffici postali). Non esiste infatti alcuna norma del Codice che impone la data certa del documento/DPS[62].Certo dimostrare che in una certa data (entro il 31 marzo di ogni anno) lo si è aggiornato costituisce una sicurezza in più; più importante è però che, in caso di controlli, l'associazione/titolare abbia un **DPS che corrisponde alle misure di sicurezza in quel momento attuate, o per lo meno che l'ultimo aggiornamento sia stato svolto nel marzo precedente**.*

*Essendo il DPS solamente un documento descrittivo della situazione dell'associazione nell'ambito della privacy, prima di stilarlo ogni associazione deve avere **un quadro completo delle misure di sicurezza adottate e da adottare**, soprattutto quelle relative agli strumenti elettronici, per il trattamento dei dati, che descriverà nel DPS medesimo.*

Per la redazione si propone un apposito **modello/esempio di DPS**[63] che ogni associazione deve adattare alla propria realtà, in base ai trattamenti informatici svolti e alle misure di sicurezza adottate.

Infine, è probabilmente da escludere che riguardi anche le Odv l'obbligo del titolare di riferire nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del DPS (p. 26 D.T.). L'art. 3 comma 3 della L. 266/91, infatti, impone all'Odv la redazione del bilancio, ma non prevede l'obbligo di una relazione accompagnatoria.

[62] Si può in ogni caso far acquisire data certa al DPS in varie modalità: a) cd. "autoprestazione" presso gli uffici postali ai sensi dell'art. 8 D.Lgs n. 261/99, con apposizione del timbro datario della Posta direttamente sul documento, anziché sulla busta, previa apposizione di francobollo di posta prioritaria e la dicitura "autoprestazione"; b) registrazione del documento presso un ufficio pubblico (Ufficio del Registro o Agenzia delle Entrate); c) autenticazione di un notaio (cfr. parere del garante 5.12.2000).
[63] Cfr. parte seconda: modelli/esempi X (DPS descrittivo) e XI (DPS schematico).

## 24. Quali sono le misure minime di sicurezza in caso di trattamento senza mezzi elettronici?

Il trattamento dei dati senza strumenti elettronici deve essere svolto adottando le seguenti misure minime di sicurezza (art. 35 Codice e nn. 27-29 D.T.):

→ **Istruzioni scritte agli incaricati** per il controllo e la custodia degli atti e documenti contenenti dati personali

*Significa che l'associazione deve stabilire le modalità di **custodia, controllo e utilizzo dei documenti** contenenti dati personali (es. se c'è un archivio, chi lo custodisce, chi può accedervi e come, ecc.), dirette ad evitare l'accesso non consentito di terzi estranei. Tali modalità si possono anche solo risolvere nel non lasciare incustoditi presso la sede atti o documenti riguardanti l'ente o gli aderenti, ma riporli in appositi armadi, eventualmente chiusi a chiave, soprattutto se si tratta di dati sensibili.*

Per tali istruzioni si può utilizzare la **lettera di incarico**[64] togliendo i riferimenti ai trattamenti elettronici.

→ L'individuazione degli **ambiti di trattamento** dei dati consentiti agli incaricati o a categorie omogenee di incaricati e il loro aggiornamento almeno annuale

*Significa che l'associazione deve stabilire per iscritto le persone o le categorie omogenee (es. volontari, es. membri del consiglio, es. dipendenti) autorizzate a compiere le attività di trattamento dei dati, con specificazione dei limiti e modalità, e verificare ed eventualmente modificare tali incarichi almeno una volta l'anno. La verifica va fatta per i casi in cui l'incaricato cessi di trattare dati (es. recesso o esclusione dell'aderente, cessazione delle cariche o degli eventuali rapporti di lavoro ecc.) o venga modificato l'ambito del suo trattamento. Per tale scritto si può utilizzare la stessa **lista degli incaricati** prevista nel caso di trattamenti elettronici[65], opportunamente modificata.*

→ L'**accesso controllato** agli archivi e documenti contenenti dati sensibili e/o giudiziari

[64] Cfr. D/R n. 21 e modello/esempio VII.
[65] Cfr. D/R n. 20 e modello/esempio XII.





*Significa che l'associazione deve far attenzione che i documenti/atti contenenti dati sensibili siano accessibili solo agli incaricati a ciò autorizzati e che costoro non lascino accedere terze persone nel corso del trattamento. L'accesso all'archivio (stanza dove stanno le banche dati cartacee) fuori dall'orario di apertura della sede deve essere registrato in un quaderno.*

*Per rendere conto dell'adozione di tali misure/procedure può essere utile (la legge non lo prevede) scrivere quello che potremmo chiamare **DPS per i trattamenti non elettronici**, per il quale si può utilizzare il **modello/esempio di DPS** [66], togliendo i riferimenti ai trattamenti elettronici.*

*Si ricordi che le associazioni che trattano dati senza strumenti elettronici devono comunque osservare gli obblighi e i limiti stabiliti dal Codice per tutti i titolari (criteri e limiti del trattamento, notifica al Garante, diritti dell'interessato, informativa ex art. 13 e consenso dell'interessato quando occorre).*

[66] Cfr. D/R n. 23 e modelli/esempio X e XI.

## 25. Quali sono le sanzioni che possono colpire l'Odv in caso di violazione delle regole della privacy?

Il mancato rispetto delle norme del Codice della privacy può comportare l'applicazione di sanzioni sia penali che amministrative, e può anche causare l'obbligo dell'associazione di risarcire i danni causati a terzi da un trattamento illegittimo. La responsabilità penale, amministrativa e civile è regolata ciascuna da principi e regole proprie.

Le principali **SANZIONI PENALI** sono:

Art. 167 – **Trattamento illecito di dati**

reclusione dai 6 ai 18 mesi per chiunque che, al fine di conseguire un proprio profitto o arrecare danno agli altri, svolge un trattamento in violazione degli art. 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, se dal fatto deriva un danno. Reclusione da 6 a 24 mesi se il fatto consiste nella comunicazione o diffusione.

*L'ipotesi più rilevante di reato consiste principalmente nell'aver causato un danno all'interessato utilizzando dati personali **senza** il suo **consenso**, quando il consenso è necessario (art. 23). Chiaramente non è illecito il trattamento senza consenso se si rientra nelle ipotesi di esclusione[67] dell'art. 24 e 26.*

reclusione da 1 a 3 anni per chiunque che, al fine di conseguire un proprio profitto o arrecare danno agli altri, svolge un trattamento in violazione degli art. 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, se dal fatto deriva un danno.

*Vengono in rilievo principalmente gli art. 25-27 che riguardano il trattamento di dati sensibili e giudiziari. Qui non è richiesto che vi sia stato un danno, è sufficiente l'utilizzo illecito di dati sensibili e giudiziari al fine di procurare danno o trarne profitto.*

Art. 168 - **Falsità nelle dichiarazioni e notificazioni al Garante**

reclusione da sei mesi a tre anni per chiunque, nella notificazione al Garante o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti,

[67] Cfr. D/R n. 13.





dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.

Art. 169 - **Misure di sicurezza**

arresto sino a due anni o ammenda da € 10.000 a € 50.000 per chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33. All'autore del reato, il Garante fissa un termine per la regolarizzazione non superiore a sei mesi. In caso di avvenuta regolarizzazione entro i 60 giorni successivi allo scadere del termine, il Garante ammette il pagamento di € 12.5000, il cui pagamento estingue il reato.

*Le norme parlano genericamente di "chiunque", ma i soggetti che rispondono del reato non sono di facile individuazione[68].*

*Soprattutto, quando il titolare è una associazione, che è una persona giuridica, sorge il problema di individuare la persona fisica responsabile penalmente, poiché la responsabilità penale può colpire solo persone fisiche, salvo casi particolari (di cui al D.Lgs. 231/01) che non riguardano la privacy.*

*A tal proposito si può dire che, all'interno dell'associazione, la responsabilità penale colpisce chi, sotto il profilo sostanziale, esercita il potere direttivo e ha preso le decisioni in materia di privacy (ad esempio ha deciso che trattamenti svolgere e le loro modalità, o ha redatto il DPS o deciso che misure minime adottare). Quindi i membri del Consiglio Direttivo, il Presidente dell'associazione, il Responsabile del trattamento o l'Amministratore di sistema eventualmente nominati sono le figure più "esposte"; il **Presidente** si potrà liberare da responsabilità dimostrando di aver conferito al Responsabile (o ad altro soggetto, ad esempio un membro del Consiglio Direttivo) deleghe effettive in materia di privacy, cioè poteri decisionali e di spesa, e dovrà probabilmente dimostrare anche di aver vigilato sull'operato del soggetto delegato. Nel caso del **Responsabile** o dell'**Amministratore di sistema** questa prova liberatoria sarà forse più difficile: egli potrà dimostrare che non gli erano state attribuite quelle funzioni il cui scorretto esercizio ha determinato il compimento di un reato, ma l'esistenza di istruzioni scritte del titolare, nel caso*

[68] I commentatori hanno sostenuto, ad esempio: che i reati di inosservanza delle prescrizioni contenute nelle autorizzazioni del Garante al trattamento dei dati sensibili (art. 26, comma 2) e la mancata adozione delle misure minime di sicurezza (art. 33) possono colpire esclusivamente il Titolare (e il Responsabile, se delegato); che il reato della mancata acquisizione del consenso (art. 23) può colpire il titolare ma anche l'incaricato, quando quest'ultimo non ha rispettato le direttive specifiche fornite dal titolare; che il reato di illecito trattamento di dati sensibili (art. 25) può essere compiuto da qualsiasi soggetto.

*del Responsabile obbligatorie per legge (cfr. art. 29), potrebbero rendere questa prova più ardua. La ripartizione delle responsabilità all'interno dell'associazione è un aspetto molto delicato: si consiglia di attribuirle in relazione all'effettiva competenza e capacità delle persone.*

*La responsabilità penale, comunque, richiede l'esistenza di vari elementi: nel caso dell'art. 167 è richiesto il dolo (cioè la volontà di commettere il reato), nel caso degli art. 168 e 169 è punita anche la colpa (ovvero la disattenzione, la noncuranza, l'imperizia, ecc.); in alcuni casi è richiesto il fine specifico (es. di arrecare danno o acquisire denaro), in altri che un danno si sia effettivamente verificato. L'accertamento della responsabilità penale comporta un'indagine svolta dal pubblico ministero, che, al termine di essa, chiede al Tribunale la condanna o l'archiviazione. Nel primo caso si svolge il giudizio davanti al Tribunale.*

*Ci si può chiedere a questo punto quale sia il* ***rischio concreto*** *per le associazioni di volontariato e gli enti non profit in genere di subire un'indagine ed eventualmente una condanna penale. La risposta non è semplice: il Pubblico Ministero, quando ha notizia di un fatto che potrebbe configurare reato, decide se indagare sulla base della gravità del fatto e dell'allarme sociale che tale fatto suscita: in questo senso è più facile che l'accertamento colpisca aziende di grandi dimensioni, o testate giornalistiche, che non una piccola associazione che utilizza un solo computer… Però teoricamente il pericolo esiste, anche in ragione del fatto che le associazioni trattano frequente dati sensibili, che sono quelli che vanno maggiormente tutelati.*

*Per le associazioni (e le Onlus in particolare) il rischio di una indagine penale potrebbe derivare principalmente dai* ***controlli della Guardia di Finanza/Agenzia delle Entrate*** *nell'accertamento del rispetto della disciplina fiscale degli enti non profit: la Guardia di Finanza agisce infatti quale pubblico ufficiale e, se riscontra la possibile esistenza di reati, ha un obbligo di denuncia alla Procura della Repubblica per gli opportuni accertamenti (art. 331 c.p.c.). Tale denuncia spetta anche al Garante ai sensi dell'art. 159, sesto comma del Codice.*

Le **SANZIONI AMMINISTRATIVE** comportano l'obbligo di pagare una somma di denaro, ed in particolare:

una somma da € 3.000 a € 18.000 quando non si trasmette all'interessato l'informativa ai sensi dell'art. 13, o il contenuto dell'informativa non è conforme a quanto prescritto dall'art. 13.





una somma da € 5.000 a € 30.000 quando non si trasmette all'interessato l'informativa ai sensi dell'art. 13, o il contenuto dell'informativa non è conforme a quanto prescritto dall'art. 13, e il trattamento riguarda dati sensibili o giudiziari o presenta rischi specifici ai sensi dell'articolo 17 o, comunque, nel caso che l'interessato abbia avuto un danno rilevante

una somma da € 5.000 a € 30.000 quando i dati sono ceduti in violazione dell'art. 16 o in violazione di altre norme del codice

una somma da € 500 a € 3.000 quando i dati sono comunicati in violazione dell'art. 84, ovvero delle regole sulla comunicazione dei dati sanitari

una somma da € 10.000 a € 60.000 in caso di mancata o incompleta notifica del trattamento al Garante ai sensi dell'art. 37 e 38

una somma da € 4.000 a € 24.000 in caso di rifiuto di fornire al Garante informazioni richieste o di esibire documenti

*Le sanzioni amministrative vengono* ***decise dal Garante per la protezione dei dati personali****, anche su reclamo o segnalazione dell'interessato, dopo una fase istruttoria di accertamento (artt. 157-160 del Codice), nella quale il Garante può chiedere al titolare, al responsabile, all'interessato o a terzi di fornire informazioni o esibire documenti. L'irrogazione della sanzione è disciplinata dalla L. 689/81: il Garante, se ritiene si sia compiuto l'illecito, notifica la contestazione; entro 60 giorni chi la riceve può far pervenire sue difese e chiedere di essere sentito; se il Garante conferma la violazione emette una ordinanza ingiunzione di pagamento, che è impugnabile davanti al giudice del luogo in cui è stato commesso l'illecito entro 30 giorni dalla notifica dell'ordinanza*[69]*.*

*La responsabilità amministrativa colpisce la persona fisica o le persone fisiche che hanno commesso la violazione (responsabili o incaricati del trattamento); la sanzione però può colpire, ai sensi dell'art. 6 L. 689/81 e a titolo di responsabilità solidale, anche:*

*a) l'associazione se l'illecito è compiuto dai suoi dipendenti;*
*b) il proprietario della cosa che è servita a commettere l'infrazione (es. l'associazione quale proprietaria del computer);*

[69] Il procedimento è lo stesso rispetto ad esempio, ad una multa per eccesso di velocità.

*c) la persona che aveva la vigilanza su chi ha commesso l'illecito, salvo non provi di non aver potuto impedire il fatto*

*In tutti questi casi, però, il responsabile solidale potrà chiedere all'autore dell'illecito l'intera somma che ha dovuto pagare (cd. azione di "regresso").*

*Altro potere del Garante è quello, previsto dall'art. 143, di imporre il blocco o la sospensione del trattamento illecito, di prescrivere al titolare l'adozione di idonee misure per renderlo lecito*.

*L'applicazione delle sanzioni amministrative è condizionata dalla gravità del fatto: se ad esempio la mancata comunicazione dell'informativa è elemento forse decisivo, in un caso di incompletezza della stessa il Garante ha ritenuto che andasse modificata ma non fosse "tale da implicare l'applicazione di una sanzione" (provv. 10.1.2002 in www.privacy.it).*

Non è finita, poiché l'associazione può anche essere colpita da **RESPONSABILITÀ CIVILE**.
L'art. 16 del Codice, infatti, prevede che

> chiunque **cagiona danno** ad altri per effetto del trattamento di dati personali è tenuto al **risarcimento** ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Significa che se l'associazione svolge con **dolo** o **colpa** un trattamento in violazione delle norme del Codice e questo trattamento causa un danno a terze persone, l'associazione con i suoi beni[70], potrà esser chiamata in causa davanti al giudice civile dal danneggiato per ottenere il risarcimento del danno patrimoniale e/o morale. Per liberarsi da responsabilità l'associazione dovrà dimostrare di aver "adottato tutte le misure idonee ad evitare il danno" (art. 2050 c.c.). Sono misure idonee sicuramente le misure minime di sicurezza, ma si ritiene che per liberarsi da responsabilità civile il titolare debba fare qualcosa di più, e cioè adottare ulteriori misure idonee[71] alla luce dello stato della tecnica, alle autorizzazioni del Garante ecc.

*Fino ad ora le (poche) pronunce dei Tribunali hanno colpito soprattutto l'illegittima pubblicazione da parte dei giornali (senza preventiva acquisizione del consenso dell'interessato) dell'immagine della persona, o di un indirizzo*

[70] E, se associazione non riconosciuta, anche le persone fisiche che hanno agito in nome e per conto dell'associazione.
[71] Cfr. D/R n. 17.





*privato, o del nominativo della vittima di un furto, ritenendo che, nei singoli casi, la pubblicazione non poteva dirsi giustificata dall'esercizio del diritto di cronaca. Si deve pertanto ritenere che qualche pericolo possa derivare alle associazioni, ad esempio, dalla diffusione del proprio giornalino, qualora qualche dato o immagine sia pubblicata senza aver ottenuto il consenso della persona: tuttavia* ***l'azione civile presuppone una iniziativa del soggetto danneggiato****, ed è abbastanza improbabile che quindi sia svolta da persone che hanno contatti "amichevoli" con l'associazione.*

## 26. Quali sono gli obblighi in caso di comunicazione dei dati all'estero o trattamento di dati provenienti dall'estero?

La comunicazione dei dati all'estero è una ipotesi non rara in ambito *non profit*, considerato che molte associazioni hanno per finalità istituzionale l'aiuto a paesi esteri o a persone che vi provengono.

L'argomento è molto vasto. Principio fondamentale è quello di cui all'art. 43 del Codice:

> Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando l'interessato ha manifestato il proprio **consenso** espresso o, se si tratta di dati sensibili, in forma scritta

Se non si ottiene il consenso il trasferimento dei dati è ugualmente possibile se ricorrono le altre ipotesi di cui all'art. 43 e 44, ed in ogni caso se l'ordinamento del Paese di destinazione o di transito dei dati assicura un livello di tutela delle persone adeguato (cd. *principio di reciprocità*). Per ulteriori approfondimenti si consiglia di esaminare gli art. da 42 a 45 del Codice.

* * *

Diverso problema è se i **dati personali di persone ed enti residenti o con sede all'estero** vengono recuperati all'estero, trasmessi in Italia e qui utilizzati da enti *non profit* italiani (es. associazioni che fanno adozioni a distanza, in genere ONG).

In questo caso si deve ritenere applicabile l'intera disciplina del Codice, che regola (art. 5) il trattamento di **dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato** (Italia).

Valgono pertanto, purtroppo (e per quanto sembri eccessivo) tutte le regole relative al trattamento di dati personali "italiani" svolto da associazioni non profit (informativa agli interessati esteri, consenso





quando è necessario, ecc.). E' vero che, quanto all'informativa, essa non è necessaria quando "comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile", ma appunto, tale esonero richiede un provvedimento espresso del Garante.

## 27. Cambia qualcosa se l'ente non profit ha rapporti con la pubblica amministrazione?

Molte Ovd ed associazioni *non profit* nello svolgimento dell'attività istituzionale instaurano rapporti con la pubblica amministrazione (es. convenzione, accreditamento, stretta collaborazione all'interno delle strutture sanitarie o socio/assistenziali) ed in ragione di questi rapporti trattano dati personali forniti dagli enti e strutture pubbliche[72].

Il Codice prevede una disciplina particolare (art. 18) quando un trattamento dei dati è svolto da un "soggetto pubblico":

> i soggetti pubblici possono trattare dati solo per lo svolgimento delle **funzioni istituzionali e, con eccezione degli esercenti le professioni sanitarie e degli organismi sanitari pubblici, non devono richiedere il consenso dell'interessato**. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Con riferimento ai dati sensibili, l'art. 20 dice che:

> Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le **finalità di rilevante interesse pubblico**[73] perseguite.

Il Codice non prevede alcuna espressa eccezione alle norme generali (descritte nelle D/R precedenti) se il trattamento è svolto da una associazione nell'ambito di un rapporto con la P.A.

[72] I trattamenti (es. ricezione dei dati dalle pubbliche amministrazioni, inserimento nelle proprie banche dati, utilizzo per lo svolgimento dell'attività istituzionale/convenzionata) riguarderanno principalmente i dati dei beneficiari dell'attività svolta in convenzione: si pensi alle associazioni che gestiscono Case Alloggio o Ceod, o seguono minori in collaborazione con il servizio sanitario…

[73] A questo proposito vale la pena citare l'art. 70 del Codice, secondo cui "si considerano di rilevante interesse pubblico, ai sensi dell'articolo 20 e 21, le finalità di applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l'elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale".



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

Viene però da chiedersi se i particolari trattamenti che riguardano l'attività in convenzione o in accreditamento devono seguire le norme del codice riferite ai soggetti privati (le associazioni sono enti privati), oppure se devono seguire le regole dettate dal Codice per i "soggetti pubblici", perché anche l'associazione si dovrebbe considerare "soggetto pubblico" quando svolga una attività "pubblica", e cioè una attività strumentale e/o finalizzata al conseguimento delle finalità pubbliche dell'amministrazione con cui collabora.

*L'argomento è difficile e incerto. Tendenzialmente si può dire che la stipula di una convenzione non modifica minimamente la natura giuridica dell'Odv o Aps o associazione, che rimane ente privato. Quando l'associazione tratta i dati personali nella sua struttura, con suoi operatori/Incaricati, con autonomia sotto il profilo gestionale e della privacy, la sua considerazione quale "soggetto pubblico" sarà assai improbabile ed essa dovrà adempiere a tutte le norme della privacy che si sono viste sopra, riferite ai soggetti privati.*

*Si aggiunga che, nell'ambito sanitario (uno di quelli dove i "contatti" con la P.A. sono più frequenti) le norme specifiche del Codice sono riferite non a qualsiasi "soggetto pubblico", ma agli "esercenti le professioni sanitarie" e agli "organismi sanitari pubblici", tra cui non possono essere certo comprese le associazioni, nemmeno se svolgono attività sanitario/assistenziale. Qualche peculiarità potrebbe presentare la situazione per cui il trattamento dei dati è svolto dall'associazione esclusivamente nell'ambito della struttura pubblica e secondo le direttive della P.A.; in questo caso l'associazione potrebbe essere considerata un "ramo" della P.A., ovvero, sotto il profilo "privacy", potrebbe essere nominata dalla P.A. (Titolare), quale Responsabile di quel trattamento*[74]*.*

*Si consiglia comunque ad ogni associazione ed ente non profit che gestisca dati forniti da enti pubblici nell'ambito di un rapporto giuridico con tali enti di definire con l'ente pubblico quali ruoli e responsabilità ciò comporta anche sotto il profilo della privacy e, nel dubbio, adottare, anche con riferimento a quel trattamento, tutte le prescrizioni del Codice relative all'informativa, al consenso, alle misure di sicurezza*[75] *adottate in generale per la sua attività.*

[74] Cfr. D/R n. 11.

[75] Peraltro, molti degli adempimenti prescritti dal Codice (informativa, misure di sicurezza….) si applicano anche ai trattamenti di dati svolti da soggetti pubblici.

## 28. Possono le Odv e gli enti *non profit* utilizzare i numeri e gli indirizzi degli elenchi telefonici per campagne di sensibilizzazione o *fundraising*? Possono utilizzare gli indirizzi e-mail o il fax o gli sms?

Molte Ovd ed enti non profit svolgono attività di sensibilizzazione e ricerca fondi inviando **comunicazioni via posta** o **chiamando al telefono** i possibili donatori privati cittadini con i dati ritrovati nell'elenco telefonico e magari inseriti nella banca dati dell'associazione.

E' consentita questa attività dopo l'entrata in vigore del Codice della privacy?

*Molto spesso si pensa che i dati contenuti negli elenchi telefonici (indirizzo dell'abitazione, numero di telefono o di fax) siano "pubblici" perché ogni persona può conoscerli facilmente, e che quindi siano liberamente utilizzabili. In realtà ciò non è vero. Sono infatti dati pubblici e quindi liberamente utilizzabili senza dover chiedere il consenso solo quei dati che sono pubblici per legge, e cioè principalmente quelli contenuti nelle liste elettorali presso i Comuni.*

I **dati contenuti negli elenchi telefonici**, invece, **sono destinati alla comunicazione interpersonale**, e quindi il loro utilizzo per fini diversi, siano essi il cd. *direct marketing commerciale* o campagne di sensibilizzazione da parte di enti *non profit*, richiede un esplicito e preventivo **consenso** dell'interessato[76].

Questa conclusione non sembra possa cambiare una volta entrato a regime il **nuovo elenco telefonico**, nel quale gli utenti possono/potranno decidere se inserire o meno il numero di telefono e/o di cellulare, l'indirizzo di casa, l'indirizzo e-mail e nei quali sarà segnalato con appositi simboli se il cittadino ha acconsentito di ricevere posta a domicilio o chiamate telefoniche o sms o mail per scopi diversi rispetto alla comunicazione interpersonale (es. offerte

[76] Il Garante, nel parere 15.7.2004 (in www.privacy.it) ha sottolineato che gli elenchi sono finalizzati solo "alla mera ricerca dell'abbonato per comunicazioni interpersonali" e che quindi un trattamento effettuato per fini ulteriori, e in particolare, per scopi pubblicitari, promozionali o commerciali, è lecito solo se è effettuato con il consenso specifico ed espresso degli interessati". In altra recente decisione del 15.6.2007 ha imposto alle società telefoniche e ai *call center* di interrompere le telefonate indesiderate e l'utilizzo dei dati acquisiti senza consenso.





pubblicitarie, propaganda elettorale e anche, appunto, iniziative di sensibilizzazione e *fundraising*).

*Il fatto che il Codice della privacy (e anche dalla Direttiva CE 58/02) non ammetta alcuna deroga per gli enti non profit, le cui campagne di raccolta fondi sono quindi in tutto e per tutto assimilate alla pubblicità (anche se perseguono fini ben più nobili), è stata la ragione, nel 2005, di varie iniziative del mondo dell'associazionismo e del non profit nei confronti del Garante per la Protezione dei Dati Personali*[77].

*Il Garante ha precisato che non esiste attualmente la possibilità di deroga a favore del non profit, e che le associazioni comunque possono, senza dover acquisire un previo consenso:*

- *utilizzare i dati delle **liste elettorali**, fornendo all'interessato la semplice informativa, poiché le campagne di fundraising hanno scopi di interesse collettivo o diffuso (art. 177 del Codice)*
- *utilizzare i dati già contenuti nelle loro banche dati, anche in questo caso fornendo l'informativa;*
- *utilizzare i dati di iscritti e aderenti per inviare campagne di sensibilizzazione, se tra scopi statutari vi sia anche la propaganda/sensibilizzazione (art. 24 e 26 del Codice)*[78].

Diverso discorso va fatto per nome della ditta/impresa e relativo indirizzo contenuti nei cd. ***elenchi categorici*** (es. *pagine gialle*, *pagine utili*). Questi dati, per loro natura commerciali, sono utilizzabili per scopi diversi dalla comunicazione personale e quindi anche per iniziative commerciali e *non profit*, senza dover richiedere un previo consenso (ma dovendo comunque trasmettere/comunicare l'informativa).

Infine, a meno che i dati non siano forniti direttamente dall'interessato, è necessario ottenere il consenso per tutte le altre particolari modalità di comunicazione elettronica, ovvero **fax, e-mail, newsletter, sms/mms** e **telefonate preregistrate**, anche se destinate ad aziende. Anche qui vale il principio di finalità, in applicazione del quale il Garante ha precisato, con specifico riferimento alla posta elettronica, che "*l'eventuale reperibilità di un indirizzo di posta elettronica sulla rete internet non lo rende per ciò stesso disponibile anche per l'invio di comunicazioni elettroniche non sollecitate*"[79].

[77] Cfr. "*Il terzo settore ha bisogno di deroghe sul diritto alla privacy*" – a cura del summit per la solidarietà, in *Terzo Settore*, n. 12/07, p. IX e X.
[78] Cfr. D/R n. 13.
[79] Cfr. decisioni del Garante 28.5.2002 e 20.4.2006 in www.privacy.it o www.garanteprivacy.it. In base a questo principio gli stessi enti *non profit* possono opporsi alle e-mail inviate da terzi che hanno

In tutti questi casi, salvo il cittadino non abbia espressamente autorizzato in elenco telefonico l'invio di materiale a fini diversi dalla comunicazione personale, sarà necessario che l'associazione invii un primo messaggio all'interessato contenente la sola richiesta di autorizzazione/consenso al trattamento.

recuperato l'indirizzo nel sito dell'associazione, indirizzo ovviamente inserito nel sito per scopi diversi da quelli della comunicazione e promozione commerciale





## 29. Esistono altri settori della privacy o casi rilevanti per il volontariato e non profit?

Il Garante per la Protezione dei Dati Personali si è spesso occupato di casi e questioni che possono riguardare anche il *non profit* e il volontariato e soprattutto gli ambiti e i settori nei quali operano.

→ nella brochure "*LA PROTEZIONE DEI DATI PERSONALI: DALLA PARTE DEL PAZIENTE*" [80] il Garante ha precisato che le associazioni di volontariato possono ricevere informazioni sui loro assistiti "*ma **devono osservare tutte le regole che le strutture sanitarie prevedono per il proprio personale interno per garantire il rispetto della dignità della persona e il massimo livello di tutela dei pazienti, nonché il segreto professionale***". Le regole di riservatezza sanitarie sono specificate dall'art. 83 del Codice (es. distanze di cortesia, postazioni di lavoro separate, ecc.). Quanto al segreto professionale, i volontari sono tenuti al rispetto di regole di condotta analoghe al segreto professionale quando trattano dati sanitari, anche se per legge non sono tenuti al segreto professionale proprio dei medici, degli infermieri, degli avvocati ecc.[81].

→ con decisione 10.4.2002 ha disposto il blocco della divulgazione tramite un sito internet dei nominativi di alunni **portatori di *handicap***, accanto ai quali era annessa una dettagliata specificazione della patologia sofferta da ciascuno;

→ in data 6.4.2006 il Garante ha espresso parere favorevole allo schema di decreto del Ministero delle Comunicazioni che ha individuato i numeri di emergenza (tra cui l'**1-1-8 di emergenza sanitaria**) nei confronti dei quali è consentita all'ente pubblico l'individuazione dell'ubicazione senza il consenso dell'utente.

[80] In www.garanteprivacy.it.

[81] La violazione del segreto professionale costituisce reato ai sensi dell'art. 622 del codice penale, compiuto da chi, "*avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da lire sessantamila a un milione*".

# GUIDA OPERATIVA DEGLI OBBLIGHI E DELLE SCADENZE

- verificare che dati personali utilizza l'associazione, a chi si riferiscono, come vengono raccolti, che natura hanno, dove vengono conservati e se vengono comunicati a terzi e/o diffusi (→ D/R n. 2 e D/R n. 4)

- verificare se l'associazione è autonomo "Titolare" del trattamento o è una sezione locale che rispetta il *sistema privacy* dell'associazione nazionale (→ D/R n. 5)

- trattare i dati in modo lecito e secondo correttezza, tutelando la riservatezza della persona o dell'ente cui i dati si riferiscono (→ D/R n. 3 e D/R n. 6) e nel rispetto delle autorizzazioni generali del Garante (→ D/R n. 15 e D/R n. 16)

- raccogliere, registrare ed utilizzare i dati solo per gli **scopi** determinati, espliciti e legittimi **indicati nello statuto** (→ D/R n. 6)
- fare in modo che i dati siano esatti, se necessario aggiornati, pertinenti, completi e non eccedenti rispetto agli scopi statutari e conservarli per un periodo di tempo non superiore a quello necessario per il raggiungimento di tali scopi, salva la possibilità di conservarli per *"fini esclusivamente personali*" (→ D/R n. 6 e D/R n. 7)
- **notificare** al Garante l'esistenza di un trattamento **solo** se l'ente è *"a carattere politico, filosofico, religioso o sindacale"* e solo se utilizza *"dati idonei a rivelare la vita sessuale o la sfera psichica"* (→ D/R n. 8)
- descrivere in una delibera di Consiglio Direttivo le modalità di utilizzo e trattamento dei dati comuni e sensibili dei soci e di coloro che hanno contatti regolari con l'associazione e richiamare tale deliberazione nell'informativa (→ D/R n. 13)



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

- fornire **l'informativa di cui all'art. 13** agli interessati che trasmettono all'ente i loro dati, e cioè ai soci/associati, ai beneficiari e terzi, ai dipendenti e collaboratori (→ D/R n. 9)
- chiedere il consenso/autorizzazione al trattamento dei dati quando richiesto (→ D/R n. 13 e D/R n. 14), previa comunicazione dell'informativa
- non chiedere il consenso ai soci/aderenti e alle persone che hanno con l'ente contatti regolari, sempre che il trattamento corrisponda agli scopi statutari e i dati non vengano comunicati a terzi o diffusi (→ D/R n. 13)
- non chiedere il consenso se si rientra nelle altre ipotesi di esclusione di cui agli art. 24 e 26 (→ D/R n. 13)
- assicurare a ogni interessato la possibilità di esercitare i **diritti di cui all'art. 7 del Codice** entro 15 giorni dalla richiesta, eventualmente nominando un Incaricato con il compito di rispondere alla richiesta medesima (→ D/R n. 10)
- eventualmente nominare un Responsabile del trattamento (→ D/R n. 11)

- in caso di **TRATTAMENTO INFORMATICO DEI DATI**, adottare le misure minime di sicurezza informatiche (→ D/R n. 17 e D/R n. 18), e cioè:
  - entro il 31 marzo di ogni anno, predisporre e aggiornare una lista degli incaricati, nominativa o per categorie di soggetti (es. volontari, soci, dirigenti, ecc.) e descrivere l'ambito del trattamento consentito a ciascun incaricato/categoria e le modalità del trattamento (cd. *sistema di autorizzazione*) (→ D/R n. 20 e D/R n. 21)
  - consegnare a ciascun incaricato una lettera di incarico nella quale descrivere l'ambito del trattamento consentito e le sue modalità (cd. *sistema di autorizzazione* (→ D/R n. 21)
  - attribuire a ciascun incaricato che utilizza computer un personale ***username*** e una ***password*** che gli consentano di accedere al computer e di svolgere i trattamenti a lui consentiti (cd. *sistema di autenticazione*) (→ D/R n. 19)

- fornire ogni computer di un idoneo **antivirus** da aggiornare almeno ogni 6 mesi, ed eventualmente di un *firewall* (→ **D/R n. 22**)
- aggiornare i sistemi operativi e i programmi dei computer (cd. *patch*) una volta all'anno in caso di trattamento di soli dati comuni o una volta ogni sei mesi in caso di trattamento di dati sensibili (→ **D/R n. 22**)
- scrivere e conservare in sede il **Documento Programmatico sulla Sicurezza** e aggiornarlo entro il **31 marzo di ogni anno** (→ **D/R n. 23**)
- salvare i dati contenuti nei computer in supporti esterni (copie di *back-up* in nastri, dischetti, CD Rom, ecc.) almeno **una volta alla settimana** → (**D/R n. 22**)
- non lasciare incustodito o accessibile il computer durante una sessione di lavoro (→ **D/R n. 22**)
- in caso di trattamento informatico di **dati sensibili**, salvare i dati in copie di *back-up* e in caso di perdita o distruzione ripristinarli entro sette giorni; distruggere i supporti esterni (es. CD rom, floppy disk) quando non sono più utilizzati e cancellare definitivamente del loro contenuto quando sono utilizzati da altri incaricati (→ **D/R n. 22**)
- Se ci si avvale di un esperto informatico esterno farsi consegnare una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Codice della *privacy* (→ **D/R n. 22**)

• in caso di **TRATTAMENTO CARTACEO** (senza computer)

- eventualmente anche mediante una **lista degli Incaricati** individuare i trattamenti consentiti agli incaricati o alle categorie di incaricati, e aggiornarla almeno una volta all'anno (→ **D/R n. 24**)
- attraverso una **lettera di incarico**, dare **istruzioni scritte agli Incaricati** sui trattamenti consentiti, sulle modalità di controllo e di custodia degli atti, dei documenti e dei fascicoli (→ **D/R n. 24**)





- controllare **l'accesso agli archivi** e ai documenti contenenti dati sensibili e/o giudiziari (→ **D/R n. 24**)

• programmare incontri formativi degli incaricati almeno una volta all'anno (→ **D/R n. 21**)

# LA SCHEDA TECNICA

(a cura di Alberto Cinetto)

Come si evince dal Disciplinare Tecnico e come già accennato nelle D/R, la scelta delle misure di sicurezza informatiche idonee ad assicurare la protezione dei dati richiede una preventiva analisi dei computer con i quali i dati vengono trattati.

Possiamo individuare a tale proposito 3 indicatori fondamentali necessari: il *tipo* di personal computer utilizzato, il *sistema operativo* installato e la presenza o meno di un *collegamento "stabile" alla rete internet*.

Si sono quindi schematizzate le varie possibilità semplificandole al massimo, in modo tale da renderle più facilmente comprensibili anche per i meno esperti. **Naturalmente tale schema è puramente indicativo** e riporta il risultato della nostra esperienza in proposito: non vuole perciò assumere valore di legge o di "prescrizione medica".

ATTENZIONE: riportiamo volutamente l'indicazione di microprocessori e sistemi operativi ormai obsoleti per testimoniare che è possibile avere un buon livello di sicurezza anche con sistemi operativi non recentissimi.

Non bisogna però dimenticare che molto spesso (per non dire sempre) risulta più conveniente tenere aggiornato il "parco macchine" piuttosto dell' "accanimento terapeutico" su PD che hanno fatto il loro tempo.

| | | |
|---|---|---|
| **Personal computer con le seguenti caratteristiche:** Processore appartenente alla categoria Celeron (600 Mhz o superiore), Athlon, Atlhon XP, Duron, Sempron, Pentium 3 e Pentium 4. Memoria Ram: 128 Mb o superiore. Sistema Operativo: Windows 95/98/ME | **Nessun collegamento a stabile a Internet** | La predisposizione di un sistema di autenticazione informatica (*username* e *password*) richiede l'installazione di un sistema operativo professionale Microsoft (Windows 2000 o Windows XP) o Linux. Si può poi prevedere un ampliamento della memoria RAM, ed è necessaria l'installazione/controllo dell'antivirus. |





| | | |
|---|---|---|
| **Personal computer con le seguenti caratteristiche:** Processore appartenente alla categoria Celeron (600 Mhz o superiore), Athlon, Atlhon XP, Duron, Sempron, Pentium 3 e Pentium 4. Memoria Ram: 128 Mb o superiore. Sistema Operativo: Windows 95/98/ME | **Collegamento stabile a Internet (ad es. ADSL)** | La predisposizione di un sistema di autenticazione informatica (*username* e *password*) richiede l'installazione di un sistema operativo professionale Microsoft (Windows 2000 o Windows XP) o Linux. Si può poi prevedere un ampliamento della memoria RAM, ed è necessaria l'installazione/controllo dell'antivirus, nonché la verifica in base ai dati trattati e alle modalità, della necessità di installazione di un router e di un firewall |
| **Personal computer con le seguenti caratteristiche:** Processore: qualsiasi Sistema Operativo: Windows NT/2000/XP Home o Professional, Windows Vista (qualsiasi versione), Mac OSX (per computer Apple Mac) | **Nessun collegamento stabile a Internet** | E' necessaria la verifica del livello di aggiornamento del sistema operativo, la verifica dell'antivirus e del sistema di autenticazione informatica (*username* e *password*). |
| **Personal computer con le seguenti caratteristiche:** Processore: qualsiasi Sistema Operativo: Windows NT/2000/XP Home o professional, Windows Vista (qualsiasi versione), Mac OSX (per computer Apple Mac) | **Collegamento stabile a Internet (ad es. ADSL** | E' necessaria la verifica del livello di aggiornamento del sistema operativo, la verifica dell'antivirus e del modem/router per l'accesso a internet, nonché, in base ai dati trattati e alle modalità, della necessità di installazione di un firewall. |
| **Personal computer con le seguenti caratteristiche:** processore 486, 386, 286 pentium, pentium II ... Sistema operativo: qualsiasi. | | Si tratta di PC molto vecchi di cui va verificata la stessa possibilità di renderli sufficientemente "sicuri". |

| | | |
|---|---|---|
| | NOTA BENE: | Ai possessori di sistemi operativi Microsoft Windows NT4 o Microsoft Windows 2000 in versione Server si consiglia l'aggiornamento a Micrrosoft Windows 2003, in quanto la casa produttrice non rilascia più aggiornamenti di sicurezza e non fornisce più supporto tecnico per i sistemi sopra citati |

*Non ci dilunghiamo sul significato e l'importanza dell'applicazione dei criteri di sicurezza che, arrivati a questo punto della pubblicazione, non dovrebbero più avere segreti per il lettore! Raccomandiamo solamente che tutte le operazioni (siano esse piccoli adeguamenti hardware oppure software) siano effettuate da personale esperto e "di fiducia" poiché nel caso in cui le necessità venissero sovrastimate vi sarebbe un inutile spreco di tempo e di denaro, nel caso invece in cui queste fossero sottostimate si verificherebbe una pericolosa esposizione ai rischi derivanti da attacchi e/o infezioni dei sistemi informatici.*





# ESEMPI / MODELLI DI DOCUMENTI

I) Informativa per volontari e/o soci
II) Informativa per beneficiari e terzi
III) Informativa per dipendenti e collaboratori
IV) Nomina a Responsabile del trattamento
V) Autorizzazione/consenso al trattamento dei dati comuni e sensibili
VI) Autorizzazione/consenso al trattamento dei dati comuni e sensibili del minore
VII) Nomina ad Incaricato del trattamento
VIII) Nota da inserire nel messaggio fax
IX) Nota da inserire nel messaggio e-mail
X) DPS descrittivo
XI) DPS schematico
XII) Lista degli Incaricati

## IMPORTANTE

E' altamente consigliato utilizzare i modelli/esempi che seguono **solo previa lettura della parte precedente** (D/R). Trattandosi di esempi e fac-simile, essi vanno compilati e se del caso modificati in base alla **situazione concreta di ogni associazione e alle modalità dei trattamenti che essa svolge**. Le parti in *corsivo* sono facoltative o sono inserite come esempi di trattamenti e situazioni frequenti nelle associazioni.

## I – ESEMPIO DI INFORMATIVA PER VOLONTARI E/O SOCI

**INFORMATIVA EX ART. 13 D. LGS. 196/03**

Gentile volontario/a /*socio*,
l'associazione tratterà i Tuoi dati personali nel rispetto del Codice della privacy (D. Lgs. 196/03), esclusivamente per lo svolgimento dell'attività istituzionale e per la gestione del rapporto associativo *(corrispondenza* e *rintracciabilità dei volontari, convocazione alle assemblee, pagamento della quota associativa e donazioni, adempimento degli obblighi di legge e assicurativi, invio del notiziario dell'associazione, informazione e sensibilizzazione*), secondo quanto stabilito con delibera del Consiglio Direttivo del …… I trattamenti saranno svolti e i dati conservati da incaricati autorizzati, in forma cartacea *e mediante computer*. *I dati non saranno comunicati a terzi né saranno diffusi. Il tuo nominativo potrà essere inserito nel notiziario dell'Associazione*.
*L'indicazione del nome, data di nascita, indirizzo, telefono e mail è necessaria per la gestione del rapporto associativo e per l'adempimento degli obblighi di legge. Il conferimento degli altri dati è facoltativo.* **Diritti dell'interessato.** Nella qualità di interessato, Ti sono garantiti tutti i diritti specificati all'art. 7 del Codice, tra cui il diritto di chiedere e ottenere dall'Associazione l'aggiornamento, la rettificazione o l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, e il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che Ti riguardano. **Titolare del trattamento** è l'associazione *di volontariato* "……", con sede a …… fax ……
***Responsabile*** *del trattamento è* ……

Il titolare

L'interessato
(per presa visione)

……
……



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

***SUGGERIMENTI***

- *Per ogni spiegazione riguardo l'informativa e il suo contenuto si legga la D/R n. 9 e inoltre le D/R n. 2, 6, 10 e 11.*
- *Questa informativa corrisponde ad un trattamento che non richiede alcuna autorizzazione/consenso del socio, poiché l'associazione non comunica i dati a terzi estranei all'associazione né li diffonde, o comunica i dati ma solo ai fini dell'adempimento degli obblighi di legge o in esecuzione di un contratto o si trova nelle altre ipotesi di esclusione del consenso.*
- *Nel caso in cui i dati vengano comunicati a terzi o diffusi e non ci siano ipotesi di esclusione del consenso è necessario ottenere l'autorizzazione/consenso del volontario e quindi far seguire all'informativa anche la richiesta di consenso (cfr. modello V).*
- *L'informativa deve distinguere i dati il cui conferimento da parte dell'interessato è obbligatorio (per il rapporto associativo) o facoltativo (es. indirizzo e-mail, studi compiuti, professione, ecc.)*
- *Nel caso l'interessato sia minorenne, si scriverà: "la nostra associazione tratterà i dati personali relativi a Suo/a figlio/a nel rispetto ……."*
- *La nomina del Responsabile è facoltativa.*
- *Firmerà l'informativa (anche solo l'originale, con consegna all'interessato della fotocopia) il legale rappresentante dell'ente*
- *L'informativa può essere trascritta sulla domanda di adesione a socio o allegata alla stessa, oppure può essere stampata su un foglio autonomo consegnato all'interessato al momento della presentazione della domanda di iscrizione (l'aspirante socio potrà firmare per presa visione la copia che rimarrà all'associazione)*

## II - ESEMPIO DI INFORMATIVA PER BENEFICIARI E TERZI

**INFORMATIVA EX ART. 13 D. LGS. 196/2003**

Gentile signora/e,
l'associazione tratterà i Suoi dati personali nel rispetto del Codice della privacy (D. Lgs. 196/03), esclusivamente per lo svolgimento dell'attività istituzionale, ed in particolare:
- *per fornire e organizzare i servizi di ……*
- *per la corrispondenza e per la rintracciabilità*
- *per l'adempimento degli obblighi assicurativi e di legge…….*
- *per ……*

I trattamenti saranno svolti da incaricati autorizzati, in forma cartacea *e mediante computer*.
*I dati non saranno comunicati a terzi né saranno diffusi.*
[oppure]
*I dati potranno esser comunicati a …… per ……*
*I dati potranno esser comunicati a …… per ……*
*Il conferimento dei dati è strumentale per il raggiungimento delle finalità dell'associazione, per l'esecuzione e l'organizzazione del servizio e per l'adempimento degli obblighi di legge*
**Dati sensibili**. Il trattamento di Suoi dati sensibili sarà effettuato nei limiti di cui alle autorizzazioni del Garante. Gli eventuali dati sanitari saranno comunicati a terzi nei limiti di quanto strettamente necessario per lo svolgimento dell'attività istituzionale, e comunque non saranno diffusi.
**Diritti dell'interessato.** Nella qualità di interessato, Le sono garantiti tutti i diritti specificati all'art. 7 del Codice, tra cui il diritto di chiedere e ottenere dall'Associazione l'aggiornamento, la rettificazione o l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, e il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano. **Titolare del trattamento** è l'associazione di volontariato "……", con sede in ……, via ……, n. ……
***Responsabile** del trattamento è* ……

Il titolare L'interessato (per presa visione)

……

……



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

***SUGGERIMENTI***

- *Per ogni spiegazione riguardo l'informativa e il suo contenuto si legga la D/R n. 9 e inoltre le D/R n. 2, 6, 10 e 11.*
- *Nel caso di beneficiari e terzi che hanno contatti regolari con l'associazione sarà sufficiente l'informativa. In caso contrario e in ogni caso se i dati vengono comunicati a terzi estranei all'associazione o diffusi sarà necessario aggiungere la richiesta di consenso (cfr. modello V).*
- *Nel caso l'interessato sia minorenne, si scriverà: "la nostra associazione tratterà i dati personali relativi a Suo/a figlio/a nel rispetto ……."*
- *Nell'informativa vanno inseriti i principali trattamenti svolti dall'associazione e la loro finalità.*
- *L'informativa deve distinguere i dati il cui conferimento da parte dell'interessato è obbligatorio o facoltativo. Un associazione che si occupa, ad esempio, di fornire un servizio di ascolto telefonico ed eventuale accompagnamento di persone anziane o in difficoltà potrà scrivere: "il conferimento dei dati anagrafici, dell'indirizzo e del numero di telefono è necessario per poterLa contattare; il conferimento di altre informazioni sulla Sua persona è facoltativo ma aiuta i volontari ad offrire un servizio migliore".*
- *La nomina del Responsabile è facoltativa.*
- *Firmerà l'informativa (anche solo l'originale, con consegna all'interessato della fotocopia) il legale rappresentante dell'ente*

## III – ESEMPIO DI INFORMATIVA PER I DIPENDENTI E COLLABORATORI

**INFORMATIVA EX ART. 13 D. LGS. 196/2003**

Con la presente siamo a comunicarLe che l'associazione "……" tratterà i Suoi dati personali nel rispetto del Codice della privacy (D. Lgs. 196/03) esclusivamente per la gestione del rapporto di lavoro o di collaborazione professionale, ed in particolare:

- *per determinare e corrispondere la retribuzione/compenso;*
- *per la corrispondenza e per la rintracciabilità;*
- *per l'adempimento degli obblighi assicurativi, di legge e di contratto;*
- *per l'adempimento degli obblighi nei confronti degli istituti di previdenza e assistenza, nonché nei confronti dell'amministrazione finanziaria;*
- *per ……*

Il trattamento sarà svolto dai incaricati autorizzati, in forma cartacea *e mediante computer*.

Il conferimento e trattamento dei dati è necessario per il raggiungimento delle finalità dell'associazione e per la gestione del rapporto di lavoro/collaborazione.

I dati saranno conservati presso …… e saranno comunicati a soggetti pubblici e privati competenti per l'esecuzione di servizi necessari per una corretta gestione del rapporto di lavoro.

I dati saranno altresì comunicati a …… per la corretta esecuzione degli obblighi di legge.

**Dati sensibili**. Il trattamento di Suoi dati sensibili, ovvero quei dati "idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché idonei a rivelare lo stato di salute e la vita sessuale", sarà effettuato nei limiti di cui alle autorizzazioni del Garante, e una volta acquisito, se necessario, il Suo consenso scritto. I dati sanitari saranno comunicati a terzi nei limiti di quanto strettamente necessario per la gestione del rapporto, e comunque non saranno diffusi.

**Diritti dell'interessato.** Nella qualità di interessato, Le sono garantiti tutti i diritti specificati all'art. 7 del Codice, tra cui il diritto di chiedere e ottenere dall'Associazione l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, e il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che La riguardano, ancorché pertinenti allo scopo della raccolta.

**Titolare del trattamento** è l'associazione *di volontariato* "……", con sede in ……, via ……, n. ……

***Responsabile** del trattamento è* ……

Il titolare

L'interessato
(per presa visione)



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

***SUGGERIMENTI***

- *Non è possibile in questa sede affrontare la complessiva disciplina della privacy riguardante i rapporti di lavoro. Per alcuni cenni, si veda la D/R n. 13. Si propone pertanto questa informativa e si rinvia alle norme specifiche del Codice: artt. 111-116*
- *La nomina del Responsabile è facoltativa.*
- *Firmerà l'informativa (anche solo l'originale, con consegna all'interessato della fotocopia) il legale rappresentante dell'ente*

## IV – ESEMPIO DI NOMINA DEL RESPONSABILE

**ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO**
**EX ART. 29 D. LGS. 196/2003**

L'Associazione "……", con sede in ……, nella persona del Presidente e legale rappresentante, in qualità di Titolare del trattamento dei dati personali

**nomina**

il signor/la signora/l'ente/la società ……, ……, Responsabile del trattamento dei dati ai sensi dell'art. 4 lett. g) e art. 29 D.Lgs. 196/03, in relazione ai trattamenti svolti all'interno dell'Associazione/*in relazione ai seguenti trattamenti:*

……
……

Nella qualità di Responsabile, ha il potere e dovere di compiere tutto quanto necessario per il rispetto e la corretta applicazione del Codice della privacy (D.Lgs. 196/03).
In particolare sono compiti del Responsabile:

- ❑ nominare per iscritto gli incaricati del trattamento impartendo loro le idonee istruzioni
- ❑ vigilare sul rispetto delle istruzioni impartite agli incaricati
- ❑ adottare le misure di sicurezza indicate e predisposte dal Titolare e vigilare sul loro buon funzionamento e corretta applicazione
- ❑ nominare, se lo ritiene opportuno, un custode delle password e un amministratore di sistema
- ❑ con l'aiuto dell'amministratore di sistema, se nominato, attribuire ad ogni incaricato le credenziali di autenticazione, e verificarne il corretto uso e sostituzione
- ❑ con l'aiuto dell'amministratore di sistema, se nominato, verificare l'efficacia delle protezioni antivirus installate
- ❑ predisporre con frequenza almeno settimanale le copie di back-up o delegare a ciò un incaricato
- ❑ organizzare uno o più incontri formativi sulla privacy per gli incaricati
- ❑ predisporre il Documento Programmatico sulla Sicurezza e portarlo all'approvazione del Consiglio Direttivo/Presidente; aggiornarlo con frequenza annuale
- ❑ rispondere tempestivamente e comunque non oltre i 15 giorni successivi al ricevimento alle richieste ed eventuali reclami degli interessati, nonché rispondere alle richieste del Garante per la protezione dei dati e dare immediata esecuzione ai provvedimenti del Garante che dovessero riguardare l'associazione
- ❑ interagire con soggetti che per legge compiono verifiche, controlli o ispezioni sulla privacy
- ❑ ……
- ❑ ……

*Per il compito assegnato il Responsabile avrà diritto al rimborso delle spese sostenute/ad un compenso pari a € …… mensili/ad un incremento stipendiale pari a € ……*

……, lì, ……





Il titolare Il Responsabile

***SUGGERIMENTI***

- *Sulla figura del Responsabile (o Responsabili) del trattamento, si veda soprattutto la D/R n. 11.*
- *Il titolare può nominare anche due o più Responsabili, fornendo a ciascuno un separato atto di nomina nel quale indicherà solo i trattamenti "affidati" a quel Responsabile.*
- *L'individuazione dei compiti e responsabilità (indicate in modo esemplificativo) va fatta sulla base della situazione concreta dell'associazione. Si consiglia la lettura delle D/R nella prima parte del libretto, ed anche del modello di DPS.*
- *Il rapporto che si instaura tra Titolare e Responsabile va probabilmente ricondotto ad un contratto di mandato (cfr. art. 1709 e seg. del codice civile). Poiché, in assenza di patti contrari, il mandato si presume oneroso, se il Titolare non intende pagare il Responsabile è meglio che lo precisi nell'atto di nomina. Sarà comunque dovuto al Responsabile il rimborso delle spese sostenute per lo svolgimento dell'incarico.*
- *Mentre nel caso dell'informativa la firma del Titolare – e cioè, per le associazioni, del soggetto cui lo statuto assegna la rappresentanza legale: il più delle volte il Presidente – va anche solo apposta nell'originale (che poi l'informativa può essere anche fotocopiata o inviata per fax, ecc.), o può anche non risultare (si pensi ad un'informativa spedita via mail), nel caso della nomina del Responsabile, che è un contratto, si deve ritenere che il Titolare debba firmare ogni atto di nomina.*
- *La firma del Responsabile per accettazione è quantomeno consigliabile (anche se probabilmente non obbligatoria), e consente al Titolare di provare di aver fornito al Responsabile le istruzioni scritte ai sensi dell'art. 29, comma 4 del Codice.*

## V – ESEMPIO DI AUTORIZZAZIONE/CONSENSO AL TRATTAMENTO DEI DATI COMUNI E SENSIBILI

**AUTORIZZAZIONE AL TRATTAMENTO DEI DATI**

Io sottoscritto/a
……

nella qualità di interessato ai sensi dell'art. 4, comma 1, lett. i) D.Lgs.n. 196/03

PRESA VISIONE DELL'INFORMATIVA RILASCIATA AI SENSI DELL'ART. 13 D.LGS. 196/03

**AUTORIZZO/DO' IL CONSENSO**

□ al trattamento dei miei **dati personali**, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del D. Lgs.n. 169/03

□ al trattamento dei miei **dati sensibili**, e nel rispetto delle disposizioni del D. Lgs. n. 169/03 e delle autorizzazioni del Garante per la Protezione dei Dati Personali e con le modalità di cui alla suddetta informativa.

……, lì ……

L'INTERESSATO
(firma leggibile)

……



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

***SUGGERIMENTI***

- *Per ogni informazione relativa al consenso si vedano principalmente le D/R n. 12, 13, 14 e 28.*
- *Se l'associazione trasmette i dati sensibili a terzi, questa circostanza deve emergere nella dichiarazione di consenso, e si potrà scrivere "al trattamento dei Suoi dati sensibili e alla loro comunicazione a terzi nei limiti e con le modalità di cui alla suddetta informativa".*

## VI – ESEMPIO DI AUTORIZZAZIONE/CONSENSO AL TRATTAMENTO DEI DATI DEL MINORE

**AUTORIZZAZIONE/CONSENSO AL TRATTAMENTO DEI DATI**

Io sottoscritto/a ……, genitore di ……, interessato al trattamento dei dati ai sensi dell'art. 4, comma 1, lett. i) D.Lgs.n. 196/03

PRESA VISIONE DELL'INFORMATIVA RILASCIATA AI SENSI DELL'ART. 13 D.LGS. 196/03

**AUTORIZZO/DO' IL CONSENSO**

❑ al trattamento dei **dati personali** di mio figlio/a, da svolgersi in conformità a quanto indicato nella suddetta informativa e nel rispetto delle disposizioni del D. Lgs.n. 169/03.

❑ al trattamento dei **dati sensibili** di mio figlio/a, da svolgersi nel rispetto delle disposizioni del D. Lgs.n. 169/03 e delle autorizzazioni del Garante per la Protezione dei Dati Personali e con le modalità di cui alla suddetta informativa.

……, lì ……

IL GENITORE
(firma leggibile)

……



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

## VII – ESEMPIO DI NOMINA AD INCARICATO

**NOMINA AD INCARICATO DEL TRATTAMENTO**

L'Associazione "……", in qualità di Titolare del trattamento dei dati personali, nella persona del Presidente e legale rappresentante,
[oppure]
*Il Responsabile del Trattamento dei dati dell'Associazione "……"*
**incarica e autorizza**
il signor/la signora ……, ……, nella qualità di "incaricato" ai sensi dell'art. 4, comma 1, lett. h) D.Lgs. 196/03, a svolgere le seguenti operazioni di trattamento all'interno dell'Associazione:
……
……
accedendo alle seguenti banche dati/archivi
……
……
**Obblighi di legge.** Nella qualità di Incaricato, dovrà svolgere i trattamenti sopra indicati esclusivamente per lo svolgimento delle mansioni e compiti affidati. Il trattamento dei dati deve essere effettuato in modo lecito e secondo correttezza. I dati devono essere esatti, pertinenti e completi, e il più possibile aggiornati, e vanno conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati. I dati potranno essere raccolti e trattati previa comunicazione dell'informativa ai sensi dell'art. 13 e, quando necessario, previa acquisizione del consenso al trattamento ai sensi dell'art. 24 e 26. In caso di cessazione del trattamento i dati dovranno essere distrutti o conservati per fini esclusivamente personali e non potranno essere destinati ad una comunicazione sistematica o alla diffusione.
**Misure di sicurezza.** L'incaricato è tenuto a rispettare le misure di sicurezza predisposte dal titolare *e dal Responsabile*.
In particolare, l'incaricato dovrà:

- ❑ non lasciare incustoditi gli atti, i documenti o il materiale che utilizza, senza la sua presenza o senza la chiusura della porta della stanza;
- ❑ conservare i dati negli appositi schedari e prelevarli per il tempo necessario al trattamento per poi riporli;
- ❑ segnalare prontamente al titolare *o al Responsabile*, con riferimento agli strumenti elettronici da lui utilizzati, ogni eventuale malfunzionamento, guasto, alterazione, errore, virus, intercettazione dei dati, accessi di terzi non autorizzati, perdita dei dati;
- ❑ ricevere le credenziali di autenticazione predisposte dal titolare/*dal Responsabile/dall'amministratore di sistema,* cambiare la password al primo accesso scegliendo una nuova password di almeno …… caratteri, non contenente elementi facilmente ricollegabili alla sua persona o all'Associazione;
- ❑ memorizzare la password e riporla in busta chiusa in un cassetto chiuso a chiave;
- ❑ sostituire la password ogni qual volta il sistema elettronico lo richiede/*ogni sei mesi*;





- ❑ non lasciare incustodito o accessibile a terzi estranei il proprio computer;
- ❑ verificare la provenienza delle e-mail, non aprire e-mail o allegati dall'incerta o pericolosa provenienza; non installare programmi scaricati da siti non ufficiali o comunque di natura incerta;
- ❑ accedere all'archivio, fuori dall'orario di lavoro/di apertura della sede, solo previa registrazione;
- ❑ seguire le istruzioni e le direttive del titolare e partecipare agli incontri di formazione programmati;
- ❑ ……
- ❑ ……

……, lì…

Il Titolare/*Responsabile*
……

l'Incaricato
(per conoscenza ed accettazione)
……

***SUGGERIMENTI***

- *Per ogni informazione relativa agli incaricati e alla loro nomina si vedano principalmente le D/R n. 2, 11, 20, 21 e 24.*
- *L'individuazione dei compiti e responsabilità dell'Incaricato (indicate in modo esemplificativo) va fatta sulla base della situazione concreta dell'associazione. Si consiglia la lettura delle D/R nella prima parte del libretto, ed anche del modello di DPS.*

## VIII – ESEMPIO DI NOTA DA INSERIRE NEL MESSAGGIO FAX

*Ai sensi e per gli effetti del D.Lgs. 196/03, questo fax è diretto esclusivamente al destinatario. Contiene pertanto informazioni riservate, tutelate dalla legge. E' vietato utilizzarne il contenuto, prenderne visione o diffonderlo senza autorizzazione. Qualora fosse da Voi ricevuto per errore vogliate cortesemente distruggerlo e, se possibile, avvertire il mittente sopra indicato.*

## IX – ESEMPIO DI NOTA DA INSERIRE NEL MESSAGGIO E-MAIL

*Ai sensi e per gli effetti del D.Lgs. 196/03, le informazioni contenute in questo messaggio e-mail sono dirette esclusivamente al destinatario, e come tali sono da considerarsi riservate. E' vietato pertanto utilizzare il contenuto dell'e-mail, prenderne visione o diffonderlo senza autorizzazione. Qualora fosse da Voi ricevuto per errore vogliate cortesemente rinviarlo al mittente e successivamente distruggerlo.*



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

## X – ESEMPIO DI DPS (DESCRITTIVO)

**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI** [82]

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, con lo scopo di descrivere il quadro delle misure minime di sicurezza, organizzative, fisiche e informatiche, da adottare e 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 ……[83]

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 ……[84], ……[85], nominato con lettera del ……[86]*

**Elenco dei trattamenti di dati personali (19.1. D.T.)**

L'associazione svolge i seguenti trattamenti di dati personali[87]:

COD1. trattamento di dati personali comuni[88] e sensibili[89] dei propri soci e/o volontari, relativi alla reperibilità ed alla corrispondenza con gli stessi o comunque necessari, funzionali o connessi alla gestione del rapporto associativo e allo svolgimento dell'attività istituzionale, per le seguenti finalità:

***SUGGERIMENTI E NOTE***
*(da cancellare una volta redatto il DPS)*

[82] *Con speciale riferimento al DPS si veda la D/R n. 23. Tuttavia la redazione del DPS presuppone lo studio di tutta la prima parte del libretto (D/R da 1 a 29).*
[83] *L'indicazione dell'attività sociale è facoltativa.*
[84] *Nome e cognome.*
[85] *Qualifica all'interno dell'associazione (es. Presidente, dipendente, volontario…..)*
[86] *Modello n. IV.*
[87] *Di seguito sono indicati i principali trattamenti che può svolgere una associazione/Odv, la natura dei dati personali e le finalità che i trattamenti possono presentare. Soprattutto le parti in corsivo sono casi ed esempi che possono anche non verificarsi: ovviamente se l'associazione non ha dipendenti o non ha collaboratori o non tratta determinati dati inserirà nel DPS solo le altre ipotesi o le ulteriori qui non delineate. Si consiglia di attribuire a ciascun trattamento un codice (un numero) da richiamare poi nelle altre parti del DPS.*
[88] *Es. nominativo, residenza, numero telefonico, indirizzo e-mail, numero di cellulare, professione, studi compiuti……*
[89] *Es. lo stesso nominativo se consente di risalire all'iscrizione all'Associazione, se questa ha carattere religioso, politico, filosofico o sindacale (cfr. D/R n. 12)*





- *creazione, organizzazione, consultazione e utilizzo di una banca dati*
- *invio del giornalino dell'associazione*
- *invio delle convocazioni alle assemblee e altre comunicazioni postali*
- *invio di messaggi di posta elettronica*
- *invio di SMS*
- *……*

COD2. trattamento di dati personali comuni[90] e sensibili[91] dei beneficiari/utenti, relativi alla reperibilità ed alla corrispondenza con gli stessi o comunque necessari, funzionali o connessi all'conseguimento delle finalità istituzionali, tra cui:

- *creazione, organizzazione, consultazione e utilizzo di una banca dati*
- *creazione di schede relative a ciascun beneficiario*
- *invio del giornalino dell'associazione*
- *campagna di sensibilizzazione attraverso l'invio di ……*
- *……*

COD3. trattamento di dati personali di fornitori, collaboratori e professionisti (*commercialisti, avvocati, consulenti del lavoro etc.*), altre organizzazioni non-profit, enti pubblici, o comunque terzi con i quali l'associazione ha periodico contatto, riguardanti la reperibilità e la corrispondenza con gli stessi, nonché richiesti ai fini fiscali o dati di natura bancaria o comunque necessari o funzionali allo svolgimento dell'attività istituzionale;

COD4. *trattamento di dati personali del personale dipendente, necessario alla gestione del rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesto ai fini fiscali o previdenziali o trattamento di dati di natura bancaria per le stesse finalità; trattamento di dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o all'adesione ad organizzazioni sindacali;*

COD5. *trattamento di dati giudiziari dei beneficiari dell'attività sociale, dipendenti o soci e/o volontari, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato, forniti dagli stessi o da terzi, necessari o conseguenti allo svolgimento dell'attività istituzionali;*

COD6. *comunicazione dei dati …… ai seguenti soggetti …….., per la finalità di ……*

COD7. *diffusione dei dati ……., mediante ……, per la finalità di ……*

[90] *Es. nominativo, residenza, numero telefonico, indirizzo e-mail, numero di cellulare, reperibilità dei parenti o delle strutture che li ospitano……*
[91] *terapia farmacologica, visite mediche o terapie da fare ……*

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.

**Strutture dove sono svolti i trattamenti, responsabili delle strutture e distribuzione dei compiti (p. 19.2. D.T.)**

*I trattamenti COD …… vengono svolti presso la sede dell'associazione, ubicata …… al …… piano di un condominio/in una casa singola/dotata di portone di ingresso con chiusura …… I singoli locali della sede dove si trovano i computer sono dotati ciascuno di porta con chiusura a chiave, così come l'archivio. La sede viene aperta ogni …… da …… e chiusa …… da ……*
*I trattamenti COD …… vengono svolti presso ……*[92]
*I trattamenti COD …… vengono svolti anche presso ……*[93]
Responsabile della struttura dove vengono svolti i trattamenti COD …… è *…… (es. il dipendente responsabile amministrativo signor …… / il Presidente dell'Associazione……); il trattamento è svolto da lui stesso e da altri soggetti incaricati (es. addetti all'amministrazione/membri del Consiglio Direttivo, volontari…)*

**Modalità dei trattamenti**

I trattamenti COD …… vengono svolti mediante i seguenti strumenti elettronici[94]:

- ❑ *1 computer con funzioni di server connesso in rete ed a internet, marca ……. modello …… contenente ……, situato presso…… Il sistema operativo del server è …… Nel server è installato il router marca …… modello ……*
- ❑ *1 computer connesso in rete ed a internet, con sistema operativo ……, contenente ……*[95]*, situato presso……*

[92] *Indicare, se ci sono, le strutture esterne alla sede dove è svolto il trattamento o anche solo la raccolta dei dati.*
[93] *Indicare, se ci sono, le strutture esterne che concorrono a svolgere il trattamento (es. studio del commercialista o del consulente del lavoro: vedi anche la parte del DPS relativa ai trattamenti affidati a soggetti esterni).*
[94] *La descrizione qui sotto è solo esemplificativa. L'associazione può anche ovviamente avere un solo computer non collegato alla rete, o non avere strumenti elettronici. Per le misure di sicurezza da adottare si veda anche la "nota tecnica".*
[95] *Indicare la banca dati esistente nel computer (es. elenco dei soci, elenco dei beneficiari……).*





- ❑ *1 computer non connesso in rete ed a internet, con sistema operativo ……, contenente ……, situato presso……*
- ❑ *1 computer portatile conservato e utilizzato da ……, con sistema operativo ……, contenente ……, situato presso……*
- ❑ *……*

*La connessione a internet è di tipo ……*

I trattamenti COD …… sono svolti *anche* mediante archivi e strumenti cartacei.

**Analisi dei rischi incombenti sui dati** (p. 19.3. D.T.)

Con riferimento alla struttura, i rischi possono consistere in ingressi di estranei a locali/aree, nella sottrazione di strumenti contenenti dati, in eventi distruttivi naturali (es. incendi, allagamenti, condizioni ambientali, ...), o artificiali (es. guasto di sistemi complementari), in errori umani nella gestione della sicurezza fisica.
*Tali rischi possono esser definiti medio/bassi, poiché la sede ha una superficie modesta, viene sempre chiusa a chiave, è sempre garantita la presenza di volontari, l'accesso di estranei è controllato costantemente ecc. ……; inoltre l'impianto elettrico è dotato di dispositivo salvavita. E' stato posto in sede un estintore.*

Con riferimento agli strumenti elettronici, i rischi possono consistere nell'azione di virus informatici o di programmi suscettibili di recare danno, nel malfunzionamento, indisponibilità o degrado degli strumenti, negli accessi esterni non autorizzati, nell'intercettazione di informazioni in rete, nella cancellazione di dati.
*I rischi possono essere definiti medi, essendo state adottate le misure di sicurezza minime, che saranno altresì costantemente aggiornate.*
*Il rischio di deterioramento e perdita dei dati può essere ritenuto basso, grazie alla conservazione di copie di sicurezza/supporti di memorizzazione in un cassetto chiuso a chiave situato nella stanza ……* [oppure] *nell'abitazione del Presidente/Responsabile……*

Con riferimento ai soggetti che trattano i dati, i rischi possono consistere nella sottrazione od uso improprio delle credenziali di autenticazione, nella carenza di consapevolezza, nella disattenzione o incuria, in errori materiali.
*A tal fine è prevista la specificazione nelle lettere di incarico dei compiti e degli accorgimenti necessari, opportuni approfondimenti in tema di sicurezza nel corso delle assemblee dei soci e lo svolgimento di corsi periodici almeno annuali…*

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

Per ridurre i rischi relativi agli strumenti elettronici verranno adottate entro il …… [oppure] sono state adottate le seguenti misure di sicurezza[96]:

- ciascun incaricato viene dotato dall'amministratore di sistema di un proprio username e di una password di …… caratteri, che va cambiata da ogni incaricato al primo accesso. La password non contiene elementi facilmente ricollegabili all'Odv o all'incaricato. *La nuova password viene memorizzata dall'incaricato e posta dall'incaricato in una busta chiusa consegnata al Responsabile/a …… e da lui custodita in un luogo che garantisca la segretezza*. *Ogni sei mesi ciascun incaricato provvederà a sostituire la propria password e a trasmetterla come sopra* [oppure] *Le password saranno modificate dall'amministratore di sistema e comunicate agli interessati ogni sei mesi.*
- si è disposto che tutti gli incaricati non lascino incustodito o accessibile il computer. *A tale riguardo, per evitare errori e dimenticanze, è stato inserito/verrà inserito lo screensaver automatico dopo …… min. di non utilizzo, con password per la prosecuzione del lavoro*[97]*.*
- Per eliminare e/o limitare il rischio di intrusione e azione di programmi (virus, trojan horse, malware, ecc.), i computer sono dotati di antivirus …… , aggiornato almeno ogni sei mesi / *con funzione di aggiornamento automatico ogni ……, ed è stato installato/sarà installato sul server/sui PC che hanno accesso a internet il <u>firewall</u> di marca ……*
- Per ogni singolo computer sarà compiuta, con scadenza semestrale, la funzione di aggiornamento del sistema operativo tramite la ditta ……[98] [oppure] mediante lo strumento windows – update
- E' stato disposto l'obbligo di provvedere alla memorizzazione delle banche dati e dei dati personali contenuti nei computer in dischetti o CD rom (cd. copie di back-up) ogni settimana; incaricato delle operazioni e della custodia dei dischetti è il Responsabile *o l'incaricato* ……
- Con riferimento ai floppy-disk ed in generale ai supporti rimovibili, se contenenti dati sensibili o giudiziari, è stato disposto che siano custoditi in cassetti chiusi a chiave e, se non più utilizzati, siano distrutti o resi inutilizzabili
- 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.

**<u>Misure di sicurezza per i trattamenti non elettronici</u>** (p. 27-29 D.T.)

Per ridurre i rischi relativi al trattamento cartaceo e manuale sono state adottate le seguenti misure:

- Si è disposto che gli incaricati non lascino incustoditi sulle scrivanie, o su altri ripiani o in luoghi accessibili all'utenza o al pubblico atti, documenti e fascicoli contenenti dati personali, ma li conservino in appositi schedari/fascicoli, prelevandoli solo per il tempo necessario al trattamento.
- Il locale destinato all'archivio sarà chiuso a chiave. Il dipendente / volontario con funzioni di custode sig. …… / il Responsabile è incaricato di controllare l'accesso all'archivio. Fuori dall'orario di apertura della sede l'accesso all'archivio sarà

[96] *Cfr. D/R n. 17 e seguenti.*
[97] *Lo screensaver con password è consigliato ma non obbligatorio.*
[98] *L'assistenza di una ditta esterna non è obbligatoria ma è una scelta dell'associazione. Cfr. sul punto D/R n. 19 e seguenti.*





consentito previa registrazione su un quaderno, qualora l'archivio contenga dati sensibili o giudiziari.

**<u>Misure per il ripristino dei dati</u>** (p. 19.5. D.T.)

Nell'ipotesi di distruzione o danneggiamento dei dati sensibili o degli strumenti elettronici che li contengono si adotterà la seguente procedura:
- gli incaricati avvertiranno il titolare*/responsabile*[99] e la persona che ha in custodia le copie di back up e i supporti elettronici contenenti i vari software installati nei computer distrutti o danneggiati;
- *il titolare/responsabile chiederà immediatamente l'intervento della ditta addetta alla manutenzione/amministratore di sistema sollecitandone al più presto l'assistenza;*
- il tecnico provvederà a reinstallare i programmi danneggiati o distrutti, o a sostituire il disco fisso o l'intero hardware, reinstallandovi il sistema operativo e i dati e programmi contenuti nelle copie di back-up e provvedendo al loro aggiornamento;
- *verrà richiesto al tecnico della manutenzione di suggerire ogni altra misura;*

In ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni dalla distruzione o danneggiamento.

**<u>Formazione degli incaricati</u>** (p. 19.6. D.T.)

La formazione degli incaricati verrà effettuata all'atto della nomina e dell'assunzione dei compiti relativi, in caso di installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Ogni incaricato riceve inoltre una lettera di incarico contenente i suoi compiti, le istruzioni operative e i limiti del suo trattamento. *Potranno essere indetti specifici corsi di una giornata, destinati a coloro i quali svolgono il trattamento di dati sensibili*. La formazione tende a sensibilizzare gli incaricati sulle tematiche della sicurezza, facendo comprendere i rischi e le responsabilità in cui incorrono (con specificazione delle sanzioni amministrative, penali e disciplinari). Inoltre, essa consiste nella spiegazione del concetto di "dato sensibile", nell'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare *e al Responsabile* ogni chiarificazione o istruzione. La formazione è svolta da ……/dal Responsabile. [100]

**<u>Trattamento da parte di soggetti esterni</u>** (p. 19.7. D.T.)

Il trattamento n. ……/il trattamento relativo a …… (*es. alla gestione delle paghe e contributi dei dipendenti dell'associazione*) è svolto all'esterno dell'associazione, avvalendosi della collaborazione del dott./rag./…… …… (*es. consulente del lavoro*).

[99] *Se nominato.*
[100] *La formazione degli incaricati è obbligatoria per legge. Se si tratta di soci/aderenti si può risolvere in una spiegazione durante l'assemblea, anche se un breve corso sarebbe l'ideale; se l'associazione ha dipendenti o personale stabile a costoro va fatta probabilmente in modo più accurato. In ogni caso, è essenziale che gli incaricati sappiano utilizzare la loro password e sappiano quali trattamenti possono svolgere e quali sono vietati. Nel fare la formazione ci si può basare sul contenuto del DPS ed eventualmente integrarlo con le più importanti nozioni contenute nella sezione D/R di questo libretto. Si ricorda che, in ogni caso, i compiti (e quindi anche i limiti) per un incaricato devono emergere nella lettera di incarico a lui consegnata (modello VII).*

Il trattamento n. ……/il trattamento relativo a …… (*es. alla gestione degli adempimenti fiscali*) è svolto all'esterno dell'associazione, avvalendosi della collaborazione del dott./…… …… (*es. commercialista*).
……

*Tali soggetti sono stati nominati Responsabili di quel specifico trattamento*[101]. Tali soggetti offrono piena garanzia per il corretto assolvimento del proprio compito, assumono l'obbligo di utilizzare i dati solo per lo scopo a loro assegnato, dichiarano di adottare le misure di sicurezza previste dal Codice e di relazionare periodicamente all'associazione sulle misure di sicurezza adottate.

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 ……[102]
……, lì

Il legale rappresentante …… *Il responsabile* ……

**N.B. CANCELLARE LE NOTE A PIE' DI PAGINA PRIMA DI STAMPARE LA VERSIONE DEFINITIVA**

[101] *La nomina del soggetto esterno quale Responsabile è facoltativa.*
[102] *L'aggiornamento del DPS deve essere svolta perlomeno entro il 31 marzo di ogni anno, quindi si potrà scrivere, ad es. "entro il 31 marzo 2008".*



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

## XI – ESEMPIO DI DPS (SCHEMATICO)

**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI** [103]

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 ……[104].

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 ……[105], ……[106], nominato con lettera del …….*

**Elenco dei trattamenti di dati personali, strutture dove sono svolti, compiti e responsabilità** (19.1. e 19.2. D.T.)

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 | | | | |

***SUGGERIMENTI E NOTE***
*(da cancellare una volta redatto il DPS)*

*[103] 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. Per la compilazione delle tabelle di questo DPS – ove lo si ritenga più comodo – si consiglia di utilizzare comunque gli esempi e le descrizioni contenute nel modello di DPS descrittivo (X).*
*[104] L'indicazione dell'attività sociale è facoltativa.*
*[105] Nome e cognome.*
*[106] Qualifica all'interno dell'associazione (es. Presidente, dipendente, volontario…..)*





| | | | | |
|---|---|---|---|---|
| COD2 | | | | |
| COD3 | | | | |
| COD4 | | | | |
| COD5 | | | | |
| ……<br>…… | | | | |

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 i dati | Dispositivi da accesso e tipologia di interconnessione | Localizzazione dei supporti di memorizzazione |
|---|---|---|---|
| COD1 | | | |
| COD2 | | | |
| COD3 | | | |
| COD4 | | | |
| COD5 | | | |
| ……<br>…… | | | |

*Società incaricata della fornitura, assistenza e manutenzione degli strumenti elettronici è ……[107], con sede …… Tale società rilascia, ai sensi del punto 25 del D.T., il certificato di conformità, che si allega al presente DPS, nel quale attesta che gli strumenti elettronici sono dotati delle misure minime di sicurezza di cui all'art. 34 T.U. e al D.T. La suddetta ditta provvede alla manutenzione dei computer, all'aggiornamento dei software e alle operazioni necessarie per consentire l'utilizzo del sistema informatico dell'associazione.*

**Analisi dei rischi incombenti sui dati** (p. 19.3. D.T.)

| 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 |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |

[107] *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"). Cfr. sul punto D/R n. 22.*





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 ……[108]
……, lì

Il legale rappresentante *Il responsabile*

……
……

**N.B. CANCELLARE LE NOTE A PIE' DI PAGINA PRIMA DI STAMPARE LA VERSIONE DEFINITIVA**

[108] *L'aggiornamento del DPS deve essere svolta perlomeno entro il 31 marzo di ogni anno, quindi si potrà scrivere, ad es. "entro il 31 marzo 2008".*



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

## XII – ESEMPIO DI LISTA DEGLI INCARICATI E MANUTENTORI

**LISTA DEGLI INCARICATI DEL TRATTAMENTO E DEI MANUTENTORI DEL SISTEMA**

L'Associazione "……", in qualità di Titolare del trattamento dei dati personali, nella persona del Presidente e legale rappresentante,
[oppure]
*Il Responsabile del Trattamento dei dati dell'Associazione "……"*

**dichiara**

che i trattamenti di dati all'interno dell'associazione descritti nel Documento Programmatico sulla Sicurezza e indicati con un codice progressivo sono svolti dai seguenti incaricati o categorie di incaricati:

COD1: *signor ……., dipendente addetto all'amministrazione/Presidente/volontari iscritti nel libro soci/……*
COD2: ……
COD3: ……

che la persona/ditta addetta alla gestione e manutenzione degli strumenti elettronici è ……, con sede in ……

Il presente documento verrà aggiornato ogni anno.

Il titolare *Il Responsabile*

…… ……

# NORMATIVA E PROVVEDIMENTI DEL GARANTE

1) Disciplinare Tecnico in materia di misure minime di sicurezza
2) Autorizzazione n. 3/2007 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni





## DISCIPLINARE TECNICO
## IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. da 33 a 36 del codice)

**Trattamenti con strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

**Sistema di autenticazione informatica**

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa

segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

**Sistema di autorizzazione**

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente**,** è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

**Altre misure di sicurezza**

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale**.**
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

**Documento programmatico sulla sicurezza**

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi





dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

**Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

**Misure di tutela e garanzia**

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

**Trattamenti senza l'ausilio di strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.





## Autorizzazione n. 3/2007 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni - 28 giugno 2007

*G.U. n. 196 del 24 agosto 2007 - supp. ord. n. 186*

Registro delle Deliberazioni
Del. n. 26 del 28 giugno 2007

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

In data odierna, con la partecipazione del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vicepresidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

Visto, in particolare, l'art. 4, comma 1, lett. *d*), del citato Codice, il quale individua i dati sensibili;

Considerato che, ai sensi dell'art. 26, comma 1, del Codice, i soggetti privati e gli enti pubblici economici possono trattare i dati sensibili solo previa autorizzazione di questa Autorità e, ove necessario, con il consenso scritto degli interessati, nell'osservanza dei presupposti e dei limiti stabiliti dal Codice, nonché dalla legge e dai regolamenti;

Visto altresì il comma 4, lett. *a*), del citato art. 26, il quale stabilisce che i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, «quando il trattamento è effettuato da associazioni, enti ed 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 dell'informativa ai sensi dell'articolo 13»;

Visto il comma 3, lettere *a*) e *b*), del predetto art. 26, il quale stabilisce che la disciplina di cui al relativo comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni; b) dei dati riguardanti Registro delle deliberazioni n. 26 del 28 giugno 2007 2 l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria;

Rilevato che le confessioni di cui alla lettera a) devono determinare, ai sensi del medesimo art. 26, comma 3, lett. *a*), idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

Visto l'art. 181, comma 6, del Codice secondo cui le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui al predetto art. 26, comma 3, lett. *a*), possono proseguire l'attività di trattamento nel rispetto delle medesime;

Considerato che il trattamento dei dati in questione può essere autorizzato dal Garante anche d'ufficio con provvedimenti di carattere generale, relativi a determinate categorie di titolari o di trattamenti (art. 40 del Codice);

Considerato che le autorizzazioni di carattere generale sinora rilasciate sono risultate uno strumento idoneo per prescrivere misure uniformi a garanzia degli interessati, rendendo altresì

superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento;
Ritenuto opportuno rilasciare nuove autorizzazioni in sostituzione di quelle in scadenza il 30 giugno 2007**,** armonizzando le prescrizioni già impartite alla luce dell'esperienza maturata;
Ritenuto opportuno che anche tali nuove autorizzazioni siano provvisorie e a tempo determinato, ai sensi dell'art. 41, comma 5, del Codice e, in particolare, efficaci per il periodo di dodici mesi;
Considerata la necessità di garantire il rispetto di alcuni principi volti a ridurre al minimo i rischi di danno o di pericolo che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali, nonché per la dignità delle persone, e in particolare, per il diritto alla protezione dei dati personali sancito dall'art. 1 del Codice;
Considerato che un elevato numero di trattamenti di dati sensibili è effettuato da enti ed organizzazioni di tipo associativo e da fondazioni, per la realizzazione di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o da un contratto collettivo;
Visto l'art. 167 del Codice;
Visto l'art. 11, comma 2, del Codice, il quale stabilisce che i dati trattati in violazione della disciplina rilevante in materia di trattamento di dati personali non possono essere utilizzati;
Visti gli articoli 31 e seguenti del Codice e il disciplinare tecnico di cui all'Allegato B) al medesimo Codice, recanti norme e regole sulle misure di sicurezza;
Visto l'art. 41 del Codice;
Visti gli atti d'ufficio;
Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
Relatore il dott. Mauro Paissan;

**Autorizza**

il trattamento dei dati sensibili di cui art. 4, comma 1, lett. *d*), del Codice da parte di associazioni, fondazioni, comitati ed altri organismi di tipo associativo, secondo le prescrizioni di seguito indicate.
Prima di iniziare o proseguire il trattamento i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalitàche permettano di identificare l'interessato solo in caso di necessità, in conformità all'art. 3 del Codice.

**1) Ambito di applicazione**

La presente autorizzazione è rilasciata:
a) alle associazioni anche non riconosciute, ai partiti e ai movimenti politici, alle associazioni e alle organizzazioni sindacali, ai patronati e alle associazioni di categoria, alle casse di previdenza, alle organizzazioni assistenziali o di volontariato, nonché alle federazioni e confederazioni nelle quali tali soggetti sono riuniti in conformità, ove esistenti, allo statuto, all'atto costitutivo o ad un contratto collettivo;
b) alle fondazioni, ai comitati e ad ogni altro ente, consorzio od organismo senza scopo di lucro, dotati o meno di personalità giuridica, ivi comprese le organizzazioni non lucrative di utilità sociale (Onlus);
c) alle cooperative sociali e alle società di mutuo soccorso di cui, rispettivamente, alle leggi 8 novembre 1991, n. 381 e 15 aprile 1886, n. 3818.
L'autorizzazione è rilasciata altresì agli istituti scolastici anche di tipo non associativo, limitatamente al trattamento dei dati idonei a rivelare le convinzioni religiose e per le operazioni strettamente necessarie per l'applicazione dell'articolo 310 del decreto legislativo 16 aprile 1994, n. 297 e degli artt. 3 e 10 del decreto legislativo 19 febbraio 2004, n. 59.





Resta fermo l'obbligo per le confessioni religiose di determinare, ai sensi dell'art. 26, comma 3, lett. *a*) del Codice, idonee garanzie relativamente ai trattamenti effettuati nel rispetto dei principi indicati con la presente autorizzazione.
Ai sensi dell'art. 181, comma 6, del Codice, le confessioni religiose che, prima dell'adozione del medesimo Codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'art. 26, comma 3, lett. *a*), del Codice possono proseguire l'attività di trattamento effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, nel rispetto delle medesime.

**2) Finalità del trattamento**

L'autorizzazione è rilasciata per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, sportive o agonistiche di tipo non professionistico, di istruzione anche con riguardo alla libertà di scelta dell'insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d'interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.
La presente autorizzazione è rilasciata, altresì, per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione nei casi previsti dalla normativa comunitaria, dalle leggi, dai regolamenti o dai contratti collettivi.
La presente autorizzazione è rilasciata per l'esercizio del diritto di accesso ai documenti amministrativi, nei limiti di quanto stabilito dalle leggi e dai regolamenti in materia.
Per i fini predetti, il trattamento dei dati sensibili può riguardare anche la tenuta di registri e scritture contabili, di elenchi, di indirizzari e di altri documenti necessari per la gestione amministrativa dell'associazione, della fondazione, del comitato o del diverso organismo, o per l'adempimento di obblighi fiscali, ovvero per la diffusione di riviste, bollettini e simili.
Qualora i soggetti di cui alle lettere a), b) e c) si avvalgano di persone giuridiche o di altri organismi con scopo di lucro o di liberi professionisti per perseguire le predette finalità, ovvero richiedano ad essi la fornitura di beni, prestazioni o servizi, la presente autorizzazione è rilasciata anche ai medesimi organismi, persone giuridiche o liberi professionisti.
I soggetti di cui alle lettere a), b) e c) possono comunicare alle persone giuridiche e agli organismi con scopo di lucro titolari di un autonomo trattamento, i soli dati sensibili strettamente indispensabili per le attività di effettivo ausilio alle predette finalità, con particolare riferimento alle generalità degli interessati e ad indirizzari, sulla base di un atto scritto che individui con precisione le informazioni comunicate, le modalità del successivo utilizzo, le particolari misure di sicurezza, nonché, ove previsto, le idonee garanzie determinate. La dichiarazione scritta di consenso degli interessati deve porre tale circostanza in particolare evidenza e deve recare la precisa menzione dei titolari del trattamento e delle finalità da essi perseguite. Le persone giuridiche e gli organismi con scopo di lucro, oltre a quanto previsto nei punti 4) e 6) in tema di pertinenza, non eccedenza e indispensabilità dei dati, possono trattare i dati così acquisiti solo per scopi di ausilio alle finalità predette, ovvero per scopi amministrativi e contabili.

**3) Interessati ai quali i dati si riferiscono**

Il trattamento può riguardare i dati sensibili attinenti:
a) agli associati, ai soci e, se strettamente indispensabile per il perseguimento delle finalità di cui al punto 1), ai relativi familiari e conviventi;
b) agli aderenti, ai sostenitori o sottoscrittori, nonché ai soggetti che presentano richiesta di ammissione o di adesione o che hanno contatti regolari con l'associazione, la fondazione o il diverso organismo;
c) ai soggetti che ricoprono cariche sociali o onorifiche;
d) ai beneficiari, agli assistiti e ai fruitori delle attività o dei servizi prestati dall'associazione o dal diverso organismo, limitatamente ai soggetti individuabili in base allo statuto o all'atto

costitutivo, 6 ove esistenti, o comunque a coloro nell'interesse dei quali i soggetti menzionati al punto 1) possono operare in base ad una previsione normativa;
e) agli studenti iscritti o che hanno presentato domanda di iscrizione agli istituti di cui al punto 1) e, qualora si tratti di minori, ai loro genitori o a chi ne esercita la potestà;
f) ai lavoratori dipendenti degli associati e dei soci, limitatamente ai dati idonei a rivelare l'adesione a sindacati, associazioni od organizzazioni a carattere sindacale e alle operazioni necessarie per adempiere a specifici obblighi derivanti da contratti collettivi anche aziendali.

**4) Categorie di dati oggetto di trattamento**

L'autorizzazione non riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale, ai quali si riferisce l'autorizzazione generale n. 2/2007.
Il trattamento può avere per oggetto gli altri dati sensibili di cui all'articolo 4, comma 1, lett. *d*) del Codice, idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.
Il trattamento può riguardare i dati e le operazioni indispensabili per perseguire le finalità di cui al punto 1) o, comunque, per adempiere ad obblighi derivanti dalla legge, dalla normativa comunitaria, dai regolamenti o dai contratti collettivi, che non possano essere perseguiti o adempiuti, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
A tal fine, anche mediante controlli periodici, deve essere verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto ai predetti obblighi e finalità, in particolare per quanto riguarda i dati che rivelano le opinioni e le intime convinzioni, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

**5) Modalità di trattamento**

Fermi restando gli obblighi previsti dagli articoli 11 e 14 del Codice, e dagli articoli 31 e seguenti del Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto alle finalità, agli scopi e agli obblighi di cui al punto 2).
I dati sono raccolti, di regola, presso l'interessato.
Fermo restando quanto previsto ai punti 2) e 7) della presente autorizzazione, se è indispensabile, in conformità al medesimo punto 7), comunicare o diffondere dati all'esterno dell'associazione, della fondazione, del comitato o del diverso organismo, il consenso scritto è acquisito previa idonea informativa resa agli interessati ai sensi dell'art. 13 del Codice, la quale deve precisare le specifiche modalità di utilizzo dei dati tenuto conto delle idonee garanzie adottate relativamente ai trattamenti effettuati.

**6) Conservazione dei dati**

Nel quadro del rispetto dell'obbligo previsto dall'art. 11, comma 1, lett. *e*) del Codice, i dati sensibili possono essere conservati per un periodo non superiore a quello necessario per perseguire le finalità e gli scopi di cui al punto 2), ovvero per adempiere agli obblighi ivi menzionati.
Le verifiche di cui al punto 4) devono riguardare anche la pertinenza, non eccedenza e indispensabilità dei dati rispetto all'attività svolta dall'interessato o al rapporto che intercorre tra l'interessato e i soggetti di cui al punto 1), tenendo presente il genere di prestazione, di beneficio o di servizio offerto all'interessato e la posizione di quest'ultimo rispetto ai soggetti stessi.

**7) Comunicazione e diffusione dei dati**

I dati sensibili possono essere comunicati a soggetti pubblici o privati, e ove necessario diffusi, solo se strettamente pertinenti alle finalità, agli scopi e agli obblighi di cui al punto 2) e tenendo presenti le altre prescrizioni sopraindicate.





I dati sensibili possono essere comunicati alle autorità competenti se necessario per finalità di prevenzione, accertamento o repressione dei reati, con l'osservanza delle norme che regolano la materia.
I dati relativi allo stato di salute e alla vita sessuale non possono essere diffusi.

**8) Richieste di autorizzazione**

I titolari dei trattamenti che rientrano nell'ambito di applicazione della presente autorizzazione non sono tenuti a presentare una richiesta di autorizzazione a questa Autorità, qualora il trattamento che si intende effettuare sia conforme alle prescrizioni suddette.
Le richieste di autorizzazione pervenute o che perverranno anche successivamente alla data di adozione del presente provvedimento, devono intendersi accolte nei termini di cui al provvedimento medesimo.
Il Garante non prenderà in considerazione richieste di autorizzazione per trattamenti da effettuarsi in difformità alle prescrizioni del presente provvedimento, salvo che, ai sensi dell'art. 41 del Codice, il loro accoglimento sia giustificato da circostanze del tutto particolari o da situazioni eccezionali non considerate nella presente autorizzazione.

**9) Norme finali**

Restano fermi gli obblighi previsti dalla normativa comunitaria, da norme di legge o di regolamento che stabiliscono divieti o limiti in materia di trattamento di dati personali.
Restano inoltre ferme le norme volte a prevenire discriminazioni, e in particolare le disposizioni contenute nel decreto-legge 26 aprile 1993, n. 122, convertito, con modificazioni, dalla legge 25 giugno 1993, n. 205, in materia di discriminazione per motivi razziali, etnici, nazionali o religiosi e di delitti di genocidio, nel decreto legislativo 9 luglio 2003, n. 215 di attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica e nel decreto legislativo 9 luglio 2003, n. 216, di attuazione della direttiva 2000/78/CE per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

**10) Efficacia temporale e disciplina transitoria**

La presente autorizzazione ha efficacia a decorrere dal 1° luglio 2007 fino al 30 giugno 2008**,** salve eventuali modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia.
La presente autorizzazione sarà pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana.
*Roma, 28 giugno 2007*
IL PRESIDENTE
Pizzetti
IL RELATORE
Paissan
SEGRETARIO GENERALE
Buttarelli

# BIBLIOGRAFIA – CENNI SULL'AUTORE e CONTRIBUTI

Il lavoro è stato costantemente confrontato con i principali commentari della L. 765/96 e del D.Lgs. 196/03, con particolare attenzione al volume "*Codice della privacy – Commento alla normativa sulla protezione dei dati personali"* di RICCARDO E ROSARIO IMPERIALI edito da IL SOLE 24ORE, ed. 2004. Per predisporre i modelli di documenti e per alcune note tecniche è stato preso spunto anche da materiale diffuso in rete (principalmente i contributi degli Avv.ti Giulia Ferrarese, Gerardo Costabile, Luca Giacopuzzi, Andrea Turco nel sito www.ilcaso.it) e da testi e riviste specificatamente dedicate al mondo del non profit, tra cui *"Terzo Settore – le regole per il non profit"* de IL SOLE 24ORE e "*Guida alla privacy nell'associazionismo*" di CARLO RIGOTTI, 2004, edito dal CSV di Trento, che si ringrazia.

Davide Cester, avvocato, è consulente legale del Centro di Servizio per il Volontariato della Provincia di Padova dal 2003. Collabora con associazioni ed enti *non profit*. In tema di privacy ha pubblicato "*Privacy, un diritto che cambia nel tempo*", in *Etica per le professioni*, Fondazione Lanza, Padova, n. 1/99.

Per la parte tecnica il lavoro è stato seguito da Alberto Cinetto, consulente informatico dal 1992 e dal 2000 direttore della Cooperativa Sociale CA2000 Onlus di Padova, che favorisce l'inserimento lavorativo di giovani con problemi di disagio familiare e sociale nel settore dell'informatica, della comunicazione e della creazione di siti web.



D. Cester – La privacy nelle associazioni di volontariato e non profit – CSV Padova

# SOMMARIO