

## **VADEMECUM ADEMPIMENTI PRIVACY GDPR 679/2016**

### **INDICE**

- 1. Cosa è cambiato**
- 2. Definizioni**
- 3. Privacy by design – privacy by default**
- 4. Principio di Accountability Art. 32 GDPR (Responsabilizzare)**
- 5. Tipologie di dati trattati dalla associazioni di volontariato**
- 6. Titolari e Responsabili del Trattamento**
- 7. Le Finalità del trattamento dei dati personali**
- 8. Le Informative redatte in base all'art. 13 GDPR**
- 9. L'Autorizzato/Incaricato del Trattamento**
- 10. Il Responsabile del Trattamento**
- 11. Il Titolare Autonomo del Trattamento**
- 12. Registro dei Trattamenti**
- 13. Obbligo di aggiornamento dei dati personali**
- 14. Il Periodo di Conservazione dei Dati**
- 15. Archivi e Albi storici dei soci**
- 16. Donazioni e Benefattori**
- 17. Diritti degli Interessati (soci, volontari, soggetti esterni, ecc.)**
- 18. I Dati Particolari (sensibili, sanitari, genetici, biometrici)**
- 19. Acquisizione del Consenso per il trattamento dei dati personali (comuni e sensibili)**
- 20. Il Consenso**
- 21. Consenso attraverso il Sito Web**
- 22. Responsabile Protezione – RPD/DPO**
- 23. Obbligo di segnalazione in caso di violazione dei dati - Data Breach**

## 1. Cosa è cambiato

Il nuovo Regolamento UE del Parlamento e del Consiglio Europeo 2016/679 detto “General Data Protection Regulation” (in breve “GDPR”) segna una ulteriore accelerazione nel campo della riservatezza e del trattamento dei dati personali.

Con la definitiva esplosione dei social network, delle piattaforme informatiche e dei motori di ricerca, le persone fisiche si comportano spesso in modo sostanzialmente opposto alla propria riservatezza, rendendo disponibili ai propri amici, al pubblico, alle imprese e alle autorità pubbliche, su scala europea e mondiale, innumerevoli informazioni personali.

La libera circolazione dei dati favorisce gli scambi, le relazioni sociali, la conoscenza, il confronto, ma cela anche vari rischi.

Il Regolamento lo dice chiaramente: il trattamento dei dati deve essere “al servizio dell’uomo”, che non deve esserne schiavo o oggetto.

Perché questo accada ogni persona deve essere posta in grado di avere il controllo su come i suoi dati, singoli o organizzati, vengono utilizzati, nell’ambito di un quadro europeo (e internazionale) di regole comuni.

Il testo della Regolamento è disponibile nel sito del Garante per la Protezione dei Dati Personali [www.garanteprivacy.it](http://www.garanteprivacy.it).

Al momento, il GDPR non ha comportato l’abrogazione dell’attuale normativa italiana (“Codice in materia di protezione dei dati personali” di cui al D.Lgs. n. 196/2003), la quale resta applicabile in tutte le norme non incompatibili con il GDPR. Sarà il legislatore italiano, in sede di emissione del Decreto Legislativo di “ratifica” del Regolamento UE, a stabilire le sorti della normativa interna (con ogni probabilità si limiterà a recepire il Regolamento, abrogando il vecchio Codice e aggiungendo la normativa di dettaglio).

## 2. Definizioni

- ☞ **DATO PERSONALE:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- ☞ **TRATTAMENTO:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione,

diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- ☞ **LIMITAZIONE DI TRATTAMENTO:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- ☞ **PROFILAZIONE:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- ☞ **PSEUDONIMIZZAZIONE:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- ☞ **ARCHIVIO:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- ☞ **TITOLARE DEL TRATTAMENTO:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- ☞ **RESPONSABILE DEL TRATTAMENTO:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- ☞ **DESTINATARIO:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- ☞ **TERZO:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- ☞ **CONSENSO DELL'INTERESSATO:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- ☞ **VIOLAZIONE DEI DATI PERSONALI:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

### 3. Privacy by design – privacy by default

La privacy deve essere vista come un elemento base delle attività dell'ente: per ogni attività dell'ente che comporta il trattamento di dati esso dovrà porsi a monte il problema di come proteggere i dati raccolti e di trattarli per il tempo e nel modo strettamente necessario per quell'attività.

Ogni ente dovrà valutare il rischio in termini di privacy legato ai trattamenti di dati effettuati e prendere le necessarie misure tecniche per proteggerli. Gli adempimenti pertanto saranno su misura per ogni soggetto a seconda dei dati trattati.

### 4. Principio di Accountability Art. 32 GDPR (Responsabilizzare)

**L'applicazione del II Principio di Accountability**, persegue l'obiettivo di **Responsabilizzare il titolare del trattamento dati**.

Il principio stabilisce che il Titolare del trattamento (l'associazione) non è più mero esecutore di un elenco di misure imposte ad una norma, ma diviene **responsabile delle misure operative e tecniche** che riterrà opportune, efficaci e dunque adeguate per salvaguardare i dati personali che tratta.

L'obiettivo di ogni titolare, responsabile e addetto al trattamento dei dati, sarà quello di **essere accountable con il regolamento**. Questo significa che il Titolare (associazione):

- ☞ deve essere responsabile delle scelte di mezzi, operazioni, procedure, finalità, ecc. in materia di trattamento dei dati,
- ☞ deve **essere in grado di "dare conto" delle valutazioni svolte alla base delle scelte poi operate.**

**ESEMPIO:** l'art.32, primo della sezione dedicata alla **sicurezza dei dati**, che recita:

- *"tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento **mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ..."**.*

☞ *Ciò comporterà che ogni soggetto dovrà autonomamente scegliere **come ed in che misura mettere in sicurezza i trattamenti** (es. quali antivirus usare);*

☞ *quali sistemi di salvataggio dei dati prevedere;*

☞ *etc.*

*Fino addirittura a poter prevedere e standardizzare procedure sulle **modalità di tenuta delle scritture degli addetti ai trattamenti** per mantenere la sicurezza dei dati cartacei.*

*Tutto questo nell'ottica moderna, introdotta dal legislatore, europeo che parte dall'idea che **nessuno, meglio del titolare, possa individuare sistemi di protezione e metodiche adeguati a garantire la sicurezza dei dati che non rallentino o impediscano le normali e quotidiane attività.***

## 5. Tipologie di dati trattati dalla associazioni di volontariato

### ***Dati Personali 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), 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 Personali Particolari (Dati Sensibili – Dati Giudiziari)***

---

L'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute (anche la semplice ferita ad una mano) o alla vita sessuale o all'orientamento sessuale della persona. Informazioni relative alle informative di garanzia e i carichi pendenti presso l'autorità giudiziaria.

Costituiscono dati personali (comuni o sensibili) anche le immagini, i suoni, i video ecc., quando consentono di individuare una persona determinata. Anche a tali dati, quindi si applicano le regole del GDPR, oltre alle norme del codice civile (art. 10) sulla tutela dell'immagine.

Le Associazioni di volontariato, o altro raccolgono e utilizzano comunemente, nello svolgimento della loro attività, dati personali, e cioè informazioni e notizie riferite:

- a. ai propri soci;
- 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. 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, 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.

## 24. Titolari e Responsabili del Trattamento

I principi del GDPR si applicano anche agli Enti del Terzo Settore, che sono “titolari del trattamento” se e ogni qualvolta svolgono operazioni di trattamento di dati personali (anche una sola volta).

Il GDPR, infatti, non si applica ai trattamenti di dati svolti da “una persona fisica per l’esercizio di attività a carattere esclusivamente personale o domestico” (es. utilizzo della rubrica telefonica nella propria abitazione), a condizione però che non si effettui una comunicazione sistematica o diffusione.

Il trattamento dei dati personali effettuato da un ente del terzo settore, pertanto, non ha fini esclusivamente personali ma a fini associativi, per il quale spesso prevede comunicazioni sistematiche, rientra nell’ambito delle applicazioni delle norme del GDPR, ed in particolare di tutte le norme applicabili agli enti privati, quali sono le associazioni e le fondazioni.

### Chi è il Titolare del Trattamento

---

**Il Titolare del trattamento è l’ente del terzo settore stesso**, sia essa associazione, fondazione o altro (definita persona giuridica), nel suo complesso, non sono titolari le persone fisiche che ne fanno parte.

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, ecc.);
- che gli adempimenti richiesti dal GDPR devono ovviamente essere attuati da persone fisiche (ad es. il Presidente, un consigliere delegato, i dipendenti, o anche i volontari);
- che i limiti imposti dal GDPR vanno rispettati da chiunque dell’associazione utilizzi dati personali;
- che, infine, le responsabilità civili, amministrative e penali in caso di violazione del GDPR gravano prevalentemente sulle persone fisiche che hanno agito.

È 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 né al RUNTS di prossima costituzione in base al Codice del Terzo Settore: le norme del GDPR che si riferiscono alle associazioni e agli enti del terzo settore, infatti, non distinguono tra i vari soggetti appartenenti al terzo settore, ma parlano genericamente di fondazioni, associazioni o organismi senza scopo di lucro.

Posto che per il GDPR il Titolare è la persona giuridica che decide che trattamento di dati svolgere e come svolgerlo (“determina le finalità e i mezzi del trattamento di dati personali”), deve esser considerata titolare del trattamento anche **la sezione locale o l’organismo periferico di una associazione**, qualora appunto eserciti un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento.

Se quindi la sezione/organismo locale di una associazione nazionale decide in autonomia in tema di privacy rispetto alla “casa madre”, va considerata “titolare”, e cioè soggetto autonomo ai fini dell’applicazione del GDPR e del rispetto degli obblighi conseguenti: deve pertanto predisporre una propria informativa, deve chiedere il consenso al trattamento, deve tenere se del caso i Registri del Trattamento e così via.

### Chi è il Responsabile del Trattamento

---

**Il Responsabile del trattamento** è la persona, che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).

Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato. Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata, dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal regolamento europeo. Inoltre dovrà garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali).

Ovviamente dovrà disporre delle risorse tecniche adeguate per l'attuazione degli obblighi derivanti dal contratto di designazione e dalle norme in materia, pertanto non può essere un soggetto interno all'associazione ma esterno all'associazione (art. 28 GDPR).

## 25. Le Finalità del trattamento dei dati personali

Ai sensi dell'art. 5 del GDPR per gli enti del terzo settore, come per qualsiasi titolare:

- Possono trattare dati personali in modo **lecito** e secondo **correttezza e trasparenza**;
- Possono raccogliere dati personali solo per **finalità** determinate, esplicite e legittime,
- Possono utilizzare dati personali solo in termini compatibili con tali scopi statuari ("**limitazione delle finalità**");
- Devono assicurarsi che i dati personali raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti ("**minimizzazione dei dati**");
- I dati personali raccolti devono essere esatti e, se necessario, costantemente aggiornati ("**esattezza dei dati**");
- I dati personali raccolti devono essere conservati per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti, a meno che la conservazione non avvenga per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ("**limitazione della conservazione**");
- Devono garantire ai dati personali raccolti un'adeguata sicurezza e protezione dei dati personali, mediante l'adozione di misure tecniche e organizzative adeguate, per evitare trattamenti non autorizzati o illeciti e per evitare la perdita e la distruzione accidentale dei dati ("**integrità e riservatezza**").

### **Principio di Finalità**

---

Il **PRINCIPIO DI FINALITÀ** è uno dei fondamenti del trattamento dei dati.

Significa che **la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate al volontario o altro soggetto (denominato Interessato).**

Per gli enti del terzo settore le finalità del trattamento dei dati generalmente coincidono o sono compresi negli **scopi istituzionali indicati nello statuto** (anche se spesso lo statuto è spesso generico, ed invece le finalità del trattamento vanno maggiormente specificate nell'informativa).

*Es. quando l'associazione raccoglie i dati personali degli 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 comunque per scopi che non riguardano l'ente.*



## 26. Le Informative redatte in base all'art. 13 GDPR

**Il GDPR obbliga gli enti del terzo settore (ODV, APS) a fornire l'informativa all'interessato.**

### Cosa è l'informativa

L'informativa è una **comunicazione** che serve per far conoscere **al volontario o altro soggetto** (denominati interessati) come il titolare gestisce e utilizza i dati che lo riguardano. È inoltre il presupposto essenziale perché l'interessato possa dare il consenso/autorizzazione al trattamento, quando questo è richiesto dalla legge.

### Cosa deve contenere l'Informativa

L'informativa deve contenere:

- a) l'identità e i dati di contatto dell'associazione (**titolare del trattamento**), ovvero, il nome dell'ente, l'indirizzo, e-mail, contatto telefonico, etc.
- b) i dati di contatto del **responsabile della protezione dei dati**, (DPO/RPD) se previsto;
- c) le **finalità** del trattamento cui sono destinati i dati personali,
- d) La **base giuridica** del trattamento, indicate nell'art. n. 6 del GDPR (*qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), devono essere indicati i legittimi interessi perseguiti dal titolare del trattamento o da terzi*);
- e) gli eventuali destinatari o le eventuali **categorie di destinatari** dei dati personali (es. associati);
- f) *l'eventuale intenzione del titolare del trattamento di trasferire dati personali in un paese terzo o ad un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili (se previsto)*;
- g) il **periodo di conservazione** dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- h) Il **diritto dell'interessato (es. associato)** di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- i) Il **diritto di revocare il consenso** in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, *qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) (dati sensibili)*,
- j) d) il diritto di proporre **reclamo** a un'autorità di controllo;

- k) e) **se la comunicazione di dati personali è un obbligo legale o contrattuale** oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l) Se è prevista la **profilazione o trattamento automatizzato**, ex art. all'articolo 22, paragrafi 1 e 4, GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

### **Informativa orale o scritta**

---

L'informativa può essere fornita **sia in forma scritta che orale**, tuttavia, poiché il titolare dovrà comunque dimostrare di averla fornita la forma migliore e più sicura per rendere l'informativa **è la forma scritta**, pertanto è evidente che la **forma scritta è consigliabile**.

### **Modalità dell'Informativa**

---

L'informativa deve avere la forma concisa, deve essere chiara, facilmente accessibile ed intellegibile per gli interessati (es. volontari), (insieme al consenso, ove richiesto) costituisce per le associazioni, soprattutto le più piccole, un'incombenza burocratica e scomoda. È utile però tener presente che:

- per quanto riguarda i **nuovi soci**, l'informativa può essere allegata o scritta sulla domanda di adesione all'associazione. 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 e-mail**. In questo caso può essere opportuno chiedere al destinatario di rinviare un messaggio di "conferma", che l'ente potrà stampare o comunque 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.

### **Modalità della comunicazione**

---


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** (definiti interessati).

La comunicazione/consegna va fatta **nel momento in cui l'interessato fornisce i suoi dati all'associazione, ovvero**, la prima volta che la persona viene a contatto con l'ente. 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.

## ***L'affissione dell'informativa nei locali dell'associazione non assolve gli obblighi di legge***

---

E' esigenza di molte associazioni (soprattutto quelle con un elevato numero di soci e con un rapido turnover) è quella di stampare un'unica informativa e renderla pubblica attraverso l'**affissione nei locali associativi**. Si tratta di una **scelta non espressamente ammessa dal GDPR!** Il Codice italiano 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 di NON adottare questa forma di comunicazione.**

## ***L'inserimento dell'informativa nello Statuto dell'Associazione***

---

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).

 **Si sconsiglia di NON adottare questa forma di comunicazione.**

## ***Pubblicazione dell'informativa sul giornale dell'associazione***

---

La pubblicazione dell'informativa **all'interno del giornale/notiziario dell'associazione** (o allegata allo stesso), se fatto pervenire direttamente agli associati, può assolvere agli obblighi imposti dal GDPR.

*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.*

L'informativa deve essere accompagnata dalla **richiesta di autorizzazione/consenso** al trattamento dei dati in tutti i casi in cui questa è da considerarsi obbligatoria, es. nei casi di dati sensibili.

## **27. L'Autorizzato/Incaricato del Trattamento**

L'incaricato/Autorizzato al Trattamento dei dati personali, è nominato dal Titolare (ente del terzo settore) ed opera sotto l'autorità diretta del titolare o del responsabile (art. 4, n. 10 GDPR).

L'incaricato/Autorizzato, è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali. L'autorizzato può operare alle dipendenze del titolare, ma anche del responsabile se nominato. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega.

L'Incaricato, per operare nel rispetto della normativa deve ricevere adeguata formazione e le istruzioni operative (art. 29 GDPR), compreso gli obblighi inerenti le misure di sicurezza (es. adozione e aggiornamento password al PC).

- ☞ In caso di mancate istruzioni anche in presenza di formali designazioni, queste sarebbero del tutto prive di valore.
- ☞ La designazione degli autorizzati può avvenire anche con unico atto per più persone.

L'eventuale designazione non necessita di firma per accettazione, anche se è utile una firma per presa visione, quale prova della conoscenza dell'incarico e delle istruzioni fornite.

L'autorizzato deve, ovviamente, attenersi strettamente alle istruzioni ricevute, e non deve avere alcuna autonomia (altrimenti è "responsabile").

Non sono previsti requisiti quantitativi per essere considerati autorizzati, per cui anche la semplice presa visione di un dato personale (es. il magazziniere che consulta la bolla di consegna, il portantino che trasporta il malato e la cartella sanitaria) si qualifica come trattamento.

Non assume alcuna rilevanza se l'incarico operi come volontario o per prestazione di lavoro e nemmeno se il collaboratore è esterno (es. il lavoratore chiamato a riparare il computer che, ovviamente, può accedere ai dati ivi contenuti) invece che inquadrato nell'azienda.

## **28. Il Responsabile del Trattamento**

Il responsabile del trattamento è la persona fisica, giuridica, o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).

Il Responsabile del Trattamento è un soggetto, diverso dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Il Titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere a responsabili che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi.

Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili

Il Responsabile del Trattamento è esterno all'azienda. Tratta i dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura. Il titolare del trattamento, ovviamente, può distribuire incarichi interni (es. responsabile dell'area legale, dell'area marketing, ecc...), ma la responsabilità rimane sua, e dell'eventuale responsabile (esterno) nominato.

## 29. Il Titolare Autonomo del Trattamento

Il **Titolare Autonomo del Trattamento**, è una figura diversa dal Responsabile, è un professionista, spesso iscritto ad albo o comunque le ipotesi in cui il fornitore esterno ha ampia autonomia e si organizza in maniera autonoma (es. commercialista, avvocato, medico del lavoro Legge 81/2008, consulente del lavoro, azienda per il DVR documento valutazione rischi),

- ☞ Il Carattere autonomo di queste figure configura il soggetto come **titolare autonomo**, diverso dal responsabile, perché non riceve istruzioni specifiche sul trattamento da parte del titolare.

## 30. Registro dei Trattamenti

Ogni ente del terzo settore che svolge un'attività di trattamento di dati personali di un certo rilievo è invitato ad istituire il Registro dei trattamenti, ex. Art. 30 del GDPR, ed è considerata indice di una corretta gestione dei trattamenti.

L'onere della tenuta del registro è a carico del titolare. La tenuta del registro costituisce uno dei principali elementi di accountability del titolare, in quanto è utile per una completa ricognizione e valutazione dei trattamenti svolti, e quindi finalizzato anche all'analisi del rischio e ad una corretta pianificazione dei trattamenti.

Per cui le autorità invitano tutti i titolari a dotarsene, eventualmente inserendo nel registro ogni elemento utile, anche oltre a quelli minimi previsti dalle norme.

Il registro, che è un documento interno, deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo (Garante) in caso di verifiche. Ovviamente il registro deve essere costantemente aggiornato.

il registro deve anche recare "in maniera verificabile" sia la data della sua prima istituzione o creazione sia la data dell'ultimo aggiornamento.

Le piccole associazioni di volontariato non sono tenute ad istituire il registro dei Trattamenti, diverso è il caso delle associazioni di grandi dimensioni, con molti volontari, dipendenti, diverse sedi, etc.

***Sono obbligate alla tenuta del registro***

---

- ☞ Le associazioni, fondazioni e comitati ove trattino “categorie particolari di dati” e/o dati relativi a condanne penali o reati (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. “vulnerabili” quali ad esempio malati, persone con disabilità, ex detenuti ecc.;
- ☞ associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull’orientamento sessuale, politico o religioso ecc.;
- ☞ associazioni sportive con riferimento ai dati sanitari trattati;
- ☞ partiti e movimenti politici;
- ☞ sindacati;
- ☞ associazioni e movimenti a carattere religioso;

### **Contenuto del Registro dei titolari del trattamento**

---

Il Registro dei Trattamenti deve consentire di identificare i soggetti coinvolti nel trattamento dei dati, le categorie dei dati trattati, per cosa sono utilizzati i dati, chi accede agli stessi, a chi vengono comunicati, per quanto tempo sono conservati e quanto sono sicuri, art. 30 GDPR.

Pertanto deve contenere:

- a. il nome e i dati di contatto del titolare del trattamento e, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati (RPD/DPO);
- b. le finalità del trattamento, distinte per tipologie (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro; trattamento dei dati di contatto dei fornitori per la gestione degli ordini);
- c. una descrizione delle categorie di interessati (es. clienti, fornitori, dipendenti) e delle categorie dei dati personali (es. dati anagrafici, dati sanitari, dati biometrici, dati genetici, dati relativi a condanne penali o reati, ecc.) trattati;
- d. i destinatari (anche solo per categoria di appartenenza) a cui i dati personali sono stati o saranno comunicati (compreso gli altri titolari, come gli enti previdenziali cui vanno trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi, ma è opportuno indicare anche i responsabili e sub-responsabili ai quali sono trasmessi i dati, come i soggetti ai quali il titolare affidi il servizio di elaborazione delle buste paga dei dipendenti);
- e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale, compresa l’identificazione del paese terzo o dell’organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell’articolo 49, la documentazione delle garanzie adeguate;
- f. dove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g. dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all’articolo 32, paragrafo 1 (è possibile fare riferimento a documenti esterni).

### **31. Obbligo di aggiornamento dei dati personali**

E’ compito dell’associazione procedere obbligatoriamente **all’aggiornamento dei dati** (art. 16 RGPD) ogni volta sia necessario per il corretto raggiungimento delle finalità del trattamento (es. dati personali

dei volontari per la compilazione del registro dei soci) 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/rettifica dei dati è anche un vero e proprio diritto dell'interessato.

## 32. Il Periodo di Conservazione dei Dati

### ***Conservazione dei dati personali***

---

Il GDPR stabilisce che la **conservazione dei dati personali** può avvenire solo se si rispettano determinate regole, ci si deve chiedere se l'associazione possa trattenere e utilizzare i dati personali dei propri associati anche dopo che essi hanno lasciato l'associazione (si tratta di un'esigenza sentita dalle associazioni, che desiderano anche solo conservare traccia di coloro che hanno "transitato" all'interno dell'ente).

La definizione del "periodo di conservazione dei dati personali" (data retention), art. 13, comma 2, lettera a del GDPR, varia in base alla tipologia di dati trattati.

👉 **Data Retention**, è il tempo di conservazione dei dati di backup, l'arco di tempo in cui un backup è disponibile per il ripristino ovvero per quanto tempo i dati salvati andranno conservati prima di essere cancellati.

La definizione del tempo di conservazione "adeguato" dipende dalla tipologia dei trattamenti. Questo tempo è dunque legato alla finalità del trattamento. Se uno stesso dato è trattato per diverse finalità, sono necessari tempi di conservazione diversi per ognuna delle diverse finalità.

### ***Utilizzo dei dati degli ex soci***

---

Il GDPR, all'art. 9 comma 2 lett. d) consente l'**utilizzo dei dati (sensibili) degli ex soci** anche senza specifico consenso, se tale utilizzo è effettuato nell'ambito dell'attività dell'associazione e con adeguate garanzie (di protezione dei dati), con **divieto però di comunicazione all'esterno** (per tale comunicazione ci vuole il consenso specifico dell'ex socio). In applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue" (es. invio della newsletter, convocazione per gli anniversari, ecc.), e quindi potranno per esempio ridursi al nominativo e all'indirizzo mail.

### ***Informazioni su tempo di conservazione nell'informativa***

---

I **tempi di conservazione** delle informazioni devono essere inseriti nell'informativa privacy che il titolare al trattamento deve fornire all'interessato "per garantire un trattamento corretto e trasparente".

Pertanto nell'informativa **ex art. 13 GDPR deve essere specificato:**

- **quali dati l'associazione intende conservare anche dopo la cessazione del rapporto associativo**, fermo restando l'avvertimento all'interessato che comunque, in ogni caso, il socio cessato potrà chiederne la cancellazione;
- dei dati del socio cessato è comunque **vietata la comunicazione all'esterno** o la diffusione (salvo esplicito consenso del socio);

### 33. Archivi e Albi storici dei soci

L'associazione con le opportune cautele per evitarne la diffusione, potrà, conservare **"l'Albo"** con i nominativi di coloro che sono stati soci, attraverso una rubrica o albo cartaceo (o attraverso lo stesso libro soci "storico") conservati in luogo non accessibile a terzi.

La conservazione dei dati dopo la cessazione del rapporto associativo è un aspetto delicato, soprattutto con riferimento a quei dati considerati "sensibili", in quanto idonei "a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale". Si capisce che la diffusione o la comunicazione a terzi di una precedente iscrizione ad una di queste associazioni, 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.

### 34. Donazioni e Benefattori

I soggetti che eseguono abitualmente o **periodicamente donazioni** all'associazione o agli enti del terzo settore, potrebbero considerarsi, ai sensi dell'art. 9 comma 2 lett. d) GDPR, persone che hanno "contatti regolari" con l'ente. In questo caso la conservazione dei dati e l'utilizzo (es. banca dati dei donatori) può avvenire senza il consenso, se i dati personali non vengono comunicati all'esterno.

- 👉 Quanto invece ai dati dei **beneficiari dell'attività**, salvo non vi siano obblighi di legge di conservazione, essi vanno cancellati quando l'attività o il servizio nei loro confronti debba intendersi definitivamente esaurito.

### 35. Diritti degli Interessati (soci, volontari, soggetti esterni, ecc.)

#### **Protezione dei Dati**

---

La protezione dei dati è assicurata all'interessato anche attraverso **l'esercizio dei diritti** indicati dagli articoli da 15 a 22 del GDPR.

In base a tali articoli **l'interessato (es. volontario) può infatti chiedere al titolare** (es. associazione):

- di avere **conferma** che l'associazione utilizza i suoi dati e di sapere **quali** siano questi **dati**;
- di conoscere l'origine dei dati (es. come e da chi l'associazione li ha acquisiti),



- le **finalità** del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati;
- di **rettificare** (correggere o integrare) i dati inesatti o incompleti (es. cambio di indirizzo o dello stato civile, aggiornamento del curriculum, ecc.);
- di **cancellare i dati** (cd. **diritto "all'oblio"**) quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR;
- di ottenere una **"limitazione del trattamento"** nei casi previsti dall'art. 18 GDPR (es. trattamento illecito dei dati);
- di poter trasferire i dati ad un altro titolare (es. da un'associazione ad altra associazione) (**diritto "alla portabilità dei dati"**) art. 20 GDPR;
- di **opporci al trattamento** dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (es. se il volontario ha presentato domanda di recesso dall'associazione o trattamento lesivo della sua dignità o riservatezza) art. 21 GDPR;
- di opporsi al trattamento dei dati svolto per il **"marketing diretto"** (es. invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale);
- di non essere sottoposto ad una decisione basata su un "trattamento automatizzato" di dati (inclusa la cd. profilazione).

☞ **Quindi ogni persona può chiedere al titolare** (es. associazione, banca, datore di lavoro, ecc.) **se e in che modo utilizza i suoi dati personali e di esercitare i suddetti diritti.**

☞ La richiesta può essere effettuata tramite posta elettronica, lettera raccomandata, fax etc.,

☞ **Consiglio: l'Associazione è invitata ad individuare una persona/Incaricato a cui attribuire il compito di occuparsi della richiesta.**

☞ Si ricordi, che gli **"interessati"** sono **principalmente gli associati/volontari**, oltre ai soggetti esterni all'associazione.

### 36. I Dati Particolari (sensibili, sanitari, genetici, biometrici)

Il GDPR all'art. 9, definisce le “**categorie particolari di dati personali**”, che consistono in:

- **DATI SENSIBILI**, che rivelano “l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale”;
- **DATI GENETICI e DATI BIOMETRICI** intesi a identificare in modo univoco una persona fisica;
- **DATI SANITARI** (e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.

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.

#### **Gli enti del terzo settore e i dati particolari**

---

**Gli enti del terzo settore possono facilmente avere a che fare con dati particolari, ovvero:**

- ☞ i dati 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 migranti).

In base all'art. 9 del GDPR si deve ritenere che sia dato “sensibile” la stessa informazione circa l'appartenenza di una persona ad una associazione che abbia carattere istituzionalmente religioso o filosofico,

- ☞ Secondo quanto stabilisce l'art. 9 del GDPR Non hanno natura “sensibile” le informazioni relative all'appartenenza alle associazioni (la maggior parte) che si richiamano genericamente a doveri e principi di solidarietà e altruismo.

### 37. Acquisizione del Consenso per il trattamento dei dati personali (comuni e sensibili)

**L'acquisizione del consenso dell'interessato (es. volontario)**, se non comporta operazioni gravose, è un'operazione che è **sempre consigliata**, anche perché al momento non è facile individuare con precisione le ipotesi di esonero dall'obbligo di chiedere il consenso al trattamento.

Con riferimento agli “enti senza scopo di lucro”, la normativa vigente prevede che il consenso non sia necessario per il trattamento di dati comuni e sensibili dei soggetti “che hanno con essi contatti regolari” o degli “aderenti”, se il trattamento è necessario “per il perseguimento di scopi determinati individuati dall'atto costitutivo, dallo statuto”, e se con l'informativa l'ente comunica all'interessato le modalità dell'utilizzo dei dati, e sempre che i dati non siano comunicati all'esterno o diffusi.

- ☞ In sostanza il Codice italiano stabilisce che **se l'ente non profit 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;**
- ☞ L'esenzione del consenso deve considerarsi esistente anche in base al GDPR, che, all'art. 9 comma 2 lett. d), **consente all'associazione l'utilizzo dei dati sensibili (e a maggior ragione dei dati personali comuni) dei "membri", "ex membri" e delle "persone che hanno regolari contatti" con l'ente, anche senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'associazione e con adeguate garanzie (di protezione dei dati);**
- ☞ **ATTENZIONE:** resta il **divieto di comunicazione all'esterno** dell'associazione **senza il consenso.**
  
- ☞ **ATTENZIONE:** Ai fini dell'esonero dal consenso, resta molto delicato definire se tra le persone che hanno "contatti regolari con l'ente" possano essere inclusi i beneficiari dell'attività che ricevono dall'associazione un servizio continuativo.

### ***Altri casi in cui è escluso il Consenso***

---

Con riferimento ai beneficiari e comunque ai non soci, possono però applicarsi agli enti del terzo settore anche altre ipotesi di esclusione del consenso previste dal GDPR.

In particolare, ai sensi dell'art. 6 GDPR, **il consenso non è richiesto quando il trattamento dei dati comuni:**

- ☞ è necessario per adempiere ad un **obbligo di legge** imposto dal diritto dell'UE o dalla legge dello Stato membro;
- ☞ è necessario per **l'esecuzione di un contratto** del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
- ☞ è necessario per **l'esecuzione di compiti di interesse pubblico;**
- ☞ è necessario per il perseguimento del legittimo **interesse dell'associazione (titolare del trattamento)** o di terzi che non leghi i diritti e le libertà fondamentali dell'interessato (es. le campagne di raccolta fondi).

*Ai sensi dell'art. 9 GDPR, il **consenso non è richiesto** quando il trattamento dei dati sensibili:*

- ☞ è necessario per gli adempimenti relativi al **diritto del lavoro, sicurezza sociale e protezione sociale;**
- ☞ è necessario per tutelare un **interesse vitale** dell'interessato o di altra persona fisica, e costoro non possano prestare il consenso;
- ☞ riguarda dati "resi manifestamente pubblici dall'interessato".

*Le norme di cui sopra consentono agli enti del terzo settore 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;*

- ☞ *se il trattamento* consiste nella comunicazione obbligatoria dei dati comuni all'Agenzia delle Entrate;
- ☞ *se il trattamento* consiste nella comunicazione dei dati comuni degli associati alla compagnia di assicurazione da parte ed enti del terzo settore iscritti ai registri del volontariato per l'assicurazione obbligatoria;
- ☞ *se il trattamento* dei dati serve per eseguire un servizio richiesto dal beneficiario (es. richiesta di trasporto o assistenza domiciliare);
- ☞ *se il trattamento* di dati sensibili serve per la tutela della vita o incolumità fisica della persona;
- ☞ *se il trattamento* di dati avviene per campagne di raccolta fondi (fermo restando il diritto dell'interessato di opporsi).

**ATTENZIONE:** tuttavia **si consiglia di chiedere il consenso ai beneficiari dell'attività se si trattano loro dati sensibili.**

### ***L'informativa sempre!***

---

***L'informativa*** che anche in caso di esonero dal consenso, **va sempre fornita** all'interessato (es. volontario)

***L'informativa***, è il documento "principe" nella gestione dei dati personali in cui sono specificate le modalità con cui l'associazione utilizza i dati

### ***Divieto assoluto di diffusione dei dati!***

---

- ☞ Vi è il divieto assoluto di diffusione (es. pubblicazione sui social) di dati sanitari e dei dati idonei a rivelare la vita sessuale neanche con il consenso dell'interessato.

## 38. Il Consenso

### **Modalità di acquisizione del Consenso al trattamento**

---

Il consenso deve essere:

- ☞ **Espresso**, cioè esplicito e manifestato in modo inequivocabile (non può essere desunto da un comportamento indiretto);
- ☞ **Libero**, cioè manifestato dall'interessato (es. volontario), richiesto in modo non definitivo.
- ☞ **Non imposto**, se il consenso è previsto in modo facoltativo (es. l'associazione non potrà imporre all'aderente di prestare il consenso al trattamento dei suoi dati per finalità estranee alle attività associative);
- ☞ **Specifico**, ovvero riferito ad uno o più trattamenti individuati e aventi specifiche finalità, e descritti con linguaggio semplice e chiaro.
- ☞  **informato**, ovvero preceduto dall'informativa di cui all'art. 13 GDPR;
- ☞ **Sempre revocabile** deve essere sempre revocabile su richiesta dell'interessato (es. volontario), tuttavia la revoca non comporta l'illegittimità dei trattamenti svolti in precedenza.
- ☞ **Dimostrabile**, il GDPR non impone sia scritto, ma impone al titolare (associazione) di **"essere in grado di dimostrare" di averlo ottenuto**, quindi è consigliabile ottenere una sottoscrizione dell'interessato o comunque conservare prova dell'avvenuta autorizzazione.

### **Accorgimenti dimostrabilità del Consenso**

---

- ☞ Per i nuovi soci/aderenti, allegare **l'informativa e il consenso** possono essere allegati **nella domanda di adesione all'associazione**, o scritti sul retro.
- ☞ **Consenso acquisito con scambio di mail**, con la richiesta all'interessato di inviare una mail (non automatica) di "conferma" (che l'ente potrà stampare e conservare), quando però gli sia stato reso chiaramente noto che il messaggio di risposta sarà inteso quale autorizzazione al trattamento.

## 39. Consenso attraverso il Sito Web

### **Modalità di acquisizione del Consenso sul sito web**

---

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 (che non sia già “preflaggate”).

Il sistema del **point&click** 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;

### ***Svantaggi del point&click***

---

L’acquisizione del consenso attraverso il web comporta 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. È pertanto consigliata solo per le grandi associazioni.

### ***Quante volte acquisire il Consenso?***

---

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 per i quali l’associazione raccoglie, registra o utilizza i dati**;
- ☞ Se l’associazione ha ottenuto il consenso nel vigore del Codice Privacy D.lgs. 196/03 **non ha l’obbligo di acquisirlo nuovamente**, a meno che i trattamenti che svolge si siano modificati in modo sostanziale da richiedere una nuova acquisizione del consenso.

L’acquisizione del consenso è abbastanza facile se l’interessato è un socio o un collaboratore dell’associazione;

Se l’interessato invece è un **beneficiario** (es. 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 in relazione ai dati personali comuni, è la sottoscrizione dell’interessato, perché consente al Titolare di dimostrare di averlo ricevuto.

### ***Il Consenso prestato dai Minori***

---

Il Consenso quando è espresso dai **minorenni**, per essere valido deve essere supportato da chi esercita la responsabilità genitoriale o dal tutore, se previsto.

Il GDPR prevede espressamente che il consenso può essere espresso validamente dai minori che abbiano raggiunto 16 anni di età, ma esclusivamente per l’offerta dei servizi della “**società dell’informazione**” (es. piattaforme web, facebook, ecc.).

- ☞ 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. **Nel dubbio è preferibile far sottoscrivere il consenso, sia per i dati comuni che per i dati sensibili**, soprattutto nei casi in cui l'associazione ha "fisicamente" la possibilità di far sottoscrivere l'interessato.

#### 40. Responsabile Protezione – RPD/DPO

L'art. 37 del GDPR introduce la una figura del "Responsabile della Protezione dei Dati" (Data Protection Officer – DPO).

Si tratta di un esperto interno o esterno all'associazione a cui spettano compiti di controllo e assistenza sui trattamenti svolti dal Titolare (Associazione), al fine di assicurare che tali trattamenti siano conformi al GDPR.

#### ***Chi è obbligato alla nomina del RPD/DPO***

---

L'art. 37 stabilisce che sono obbligati a nominare il Responsabile della Protezione dati:

- ☞ Gli **enti pubblici** (Comune, Scuole, Provincia, ASL, etc.);
- ☞ I **Titolari privati (es. aziende)** che hanno come attività principale lo svolgimento di "trattamenti che, per loro natura, ambito o finalità, richiedono il **monitoraggio regolare** e sistematico degli interessati su larga scala";
- ☞ I Titolari privati la cui attività principale consiste "nel trattamento, su larga scala, di **categorie particolari** di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

**ATTENZIONE:** Sono tenuti alla nomina del DPO solo gli enti del terzo settore che, nello svolgimento della loro attività principale, svolgono un monitoraggio sistematico SU LARGA SCALA dei beneficiari/destinatari della loro attività o compiono un trattamento SU LARGA scala di dati sensibili o giudiziari.

#### ***Trattamento su larga scale***

---

Un trattamento di dati è svolto "SU LARGA SCALA" quando vi è un elevato numero di interessati (es. associazione con diverse sedi sul territorio, oppure, un elevato numero di interessati, o elevato numero di dati personali).

Le Linee Guida europee (Article 29 Data Protection Working Party) hanno indicato a titolo esemplificativo come soggetti che svolgono trattamenti su vasta scala gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione, ecc.

## 41. Obbligo di segnalazione in caso di violazione dei dati - Data Breach nel GDPR

Il **Data Breach** è la violazione dei dati personali che si può verificare durante le operazioni di trattamento.

- ☞ La violazione dei dati personali si può verificare accidentalmente o per trattamento illecito
- ☞ Conseguenza del Data Breach può essere la distruzione, la perdita, la modifica, la divulgazione non autorizzata di dati personali, l'accesso ai dati personali.

### **Notifica Data Breach**

---

Nel caso in cui si dovesse verificare una delle ipotesi di Data Breach, il Titolare (associazione, ente del terzo settore) deve procedere alla notifica on-line della violazione al Garante per la Protezione dei Dati Personali.

- ☞ La notifica della violazione va fatta entro il più breve tempo possibile e comunque senza ingiustificato ritardo entro 72 ore successive al momento in cui si è venuti a conoscenza della violazione. L'eventuale ritardo dovrà essere motivato
- ☞ Il Titolare (es. associazione) si può esimere dalla notifica, se è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone.

### **Istituzione del registro di Data Breach**

---

L'associazione è invitata ad istituire il Registro dei casi di data breach, sia dei casi di violazione effettivamente occorsi sia per le minacce potenziali, per identificare il tipo e la natura delle violazioni più ricorrenti.

### **Contenuto della Notifica**

---

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR, ovvero:

- ☞ **descrivere** la natura della violazione dei dati personali compresi, se possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- ☞ **comunicare** il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- ☞ **descrivere** le probabili conseguenze della violazione dei dati personali;
- ☞ **descrivere** le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La notifica va effettuata via PEC all'indirizzo [protocollo@pec.gdpd.it](mailto:protocollo@pec.gdpd.it). L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.