CSV LAZIO
Centro di Servizio per il Volontariato

GDPR

Per ulteriori approfondimenti si rimanda a:

- Testo del GDPR [https://bit.ly/2UUX5Ky]
- Decreto 101/18 [https://bit.ly/2M8D5hZ]
- Intervista: CSV Lazio e il GDPR https://bit.ly/2RbBZsE
- *GDPR Lo stretto indispensabile per le organizzazioni del Volontariato*, Amazon [http://amzn.eu/d/jeZMFbH]

Editore: CSV Lazio, via Liberiana 17, Roma

Autore: Alberto Pattono; Editing In Pagina sas Milano

Stampato nel novembre 2018 da

Indice

Introduzione

Una nuova sfida si è aperta con l'approvazione del Regolamento generale sulla Protezione dei Dati personali (RGDP) e sempre di più siamo consapevoli che è necessario mobilitarsi davanti a questa prova e fare, di queste nuove norme, un'occasione di crescita.
Questo processo investe tutti, le pubbliche amministrazioni, i grandi enti e le piccole associazioni che, raccogliendo dati personali, devono organizzarsi in modo nuovo per trattarli e custodirli nella maniera più adeguata .
Nei mesi trascorsi si è aperto dunque un confronto anche nel CSV Lazio per comprendere quali fossero le strategie migliori da attivare e quali indicazioni fornire alle associazioni che ponevano alcune domande.
Affidarsi ad esperti a pagamento o a titolo gratuito per fargli fare il lavoro per conto dell'Associazione? Con quali prospettive e soprattutto risorse?
La strada intrapresa, che è sembrata inizialmente più complessa ma certamente più utile, è stata quella di sostenere le associazioni in un percorso di crescita attraverso il quale capire non solo la norma, ma anche le ragioni per cui era stata formulata, appropriarsene, farla diventare un'abitudine di lavoro corretto, facendo crescere così trasparenza e fiducia nell'Associazione.
Abbiamo infatti immaginato che raccogliere la sfida poteva servire ad una crescita culturale: non si tratta tanto di applicare procedure burocratiche, quanto di essere più consapevoli dei dati che raccogliamo e gestiamo e delle conseguenti responsabilità che abbiamo nei confronti delle persone con le quali e per le quali lavoriamo.

Un compito che all'inizio può sembrare difficile, ma che con un po' di buona volontà può diventare abitudine consolidata.
Per queste ragioni il CSV Lazio ha programmato alcune azioni di supporto alle associazioni, perché acquisissero le competenze necessarie, a diversi livelli: incontri informativi/formativi in tutti i territori della Regione Lazio; un supporto di consulenza alle associazioni che hanno frequentato il corso per una verifica della documentazione prodotta; la pubblicazione di questa guida introduttiva per diffondere il più possibile, ed in modo speriamo semplice, tutte le azioni che le associazioni devono attivare per il trattamento dei dati personali.
Resta il fatto che il CSV può dare un servizio, ma l'Associazione deve lavorare prima (capire i trattamenti e raccogliere le informazioni) e dopo (adattare alla propria realtà le indicazioni e i moduli base forniti dal CSV), considerando questo adempimento non una "pratica da sistemare" ma un investimento che l'aiuterà a crescere.

Paola Capoleva
Renzo Razzano

GDPR: che cos'è? Perché ci riguarda da vicino?

Nel 2016 il Parlamento Europeo ha approvato una legge, per l'esattezza un Regolamento Europeo entrato in pieno vigore nel maggio 2018 che ha rivoluzionato la raccolta e la gestione dei dati personali in tutti i Paesi dell'Unione Europea.
In inglese si chiama General Data Protection Regulation (GDPR), in italiano Regolamento generale sulla protezione dei dati (RGDP). Si chiama anche Regolamento UE 2016/679. Qui usiamo la sigla GDPR più spesso usata anche in Italia.
Nessuna 'esenzione'. Le Associazioni, anche le più piccole, sono soggette a questa normativa. Il GDPR si applica a realtà di qualsiasi dimensione, né fa alcuna distinzione fra realtà con e senza fine di lucro. No profit nel mirino. Il terzo settore è coinvolto dal GDPR più ancora delle imprese. Il GDPR si occupa della protezione dei dati delle persone fisiche. La maggior parte delle aziende lavora con altre aziende e quindi con persone giuridiche. Certo, queste relazioni coinvolgono persone, ma solo come mezzo attraverso il quale le aziende entrano in contatto fra loro. Le organizzazioni del terzo settore invece 'nuotano' nei dati personali. Soci, volontari, donatori, assistiti...
Non solo per paura delle sanzioni. Il GDPR è una delle leggi alle quali è necessario adeguarsi. Prevede delle sanzioni con dei massimi pesantissimi, milioni di euro. In realtà non è probabile che una realtà del terzo settore sia colpita da una sanzione a causa del GDPR. L'Autorità Garante dei dati personali che potrebbe farlo, si concentrerà sui casi più eclatanti di traffico e furto di dati personali.

Prevenire le richieste dei partner istituzionali. Invece è molto probabile che l'adeguamento al GDPR sia presto richiesto come prerequisito da enti pubblici e dai grandi donatori.
Molte realtà del Terzo settore stringono convenzioni, utilizzano spazi, condividono informazioni con Ospedali, Comuni, Regioni o altre Amministrazioni. Queste realtà, una volta che si saranno messe a norma, avranno ben ragione di chiedere alle Associazioni di documentare la loro adesione al GDPR. E lo stesso potrebbero fare, già accade, Fondazioni e Aziende.
Rendere più trasparente l'operato dell'Associazione. Come vedremo, rispettare il GDPR significa documentare il proprio modo di lavorare, renderlo leggibile e trasparente.
Questa trasparenza spesso nelle organizzazioni del terzo settore è un aspetto migliorabile. La documentazione GDPR si rivelerà utile per un volontario che vuole entrare a far parte del Direttivo o in caso di successione alla guida dell'Associazione, o anche solo per informare un socio che vuole saperne di più.
Una questione di rispetto. Si tratta di garantire i soci e i volontari, i donatori e gli assistiti che l'organizzazione prende sul serio, non la norma in sé, ma la loro privacy, la rispetta anche su questo fronte.
È vero che noi italiani non siamo molto attenti alla privacy, condividiamo i nostri dati personali senza troppo pensarci. Ma lo stesso avveniva anche per i contributi. Ieri donavamo a questa o a quella Associazione 'sulla fiducia' oggi vogliamo sapere precisamente (o comunque ci fa piacere sapere) come saranno utilizzati i nostri soldi. Quindi sempre di più sarà utile rendere esplicite le modalità di trattamento dei dati personali anche per aumentare la "fiducia" verso l'Associazione.

Cosa bisogna fare? Chi deve farlo? Quando?

Cosa fare. A differenza del modello giuridico cui siamo abituati: "queste sono le cose da fare, se succede qualcosa, ti sanziono"; le norme europee dicono: "se succede qualcosa, tu devi solo dimostrare di aver fatto il possibile per evitarlo". Quindi in sintesi il GDPR chiede di:

- descrivere l'utilizzo che si fa dei dati personali di cui si dispone;
- tenere presenti i rischi e l'impatto sulla privacy della persona e di operare per ridurli al minimo;
- informare le persone.

Chi deve farlo. Il compito di allestire questa documentazione non può essere delegato in toto a un professionista o al CSV. Chi si è rivolto a professionisti esterni ha ricevuto documentazioni molto vaghe o imprecise sul piano sostanziale. Un esterno non può descrivere come funziona la vostra organizzazione. Può aiutare nell'identificare i trattamenti, può proporre dei testi base che l'organizzazione adatterà, può identificare e risolvere alcuni aspetti critici. Ma l'organizzazione dovrà dedicare del tempo per affrontare il GDPR.

Quando. Il GDPR è pienamente operativo dal 25 maggio 2018, ci sono state alcune 'quasi proroghe' che sono comunque scadute. Questo non significa che sia troppo tardi per adeguarsi. Di fatto la gran parte delle amministrazioni si metterà in regola entro la fine del 2018 o nei primi mesi del 2019. Quindi essere partiti in ritardo non è una ragione per non adeguarsi il prima possibile. Non è mai troppo tardi.

Le parole chiave

Per proseguire occorre chiarire alcuni concetti e termini chiave.

Dati personali. Per dati personali si intende "qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica". Quindi ogni tipo di informazione che possa essere riconducibile, anche senza certezza, a una persona fisica. Ovviamente i dati anagrafici, gli indirizzi, le informazioni riguardanti la salute. Sono dati personali la corrispondenza cartacea o elettronica e le immagini che ritraggono una persona, tutti i dati che permettono di associarla a una posizione nello spazio e nel tempo, gli accessi a un sito web.

Trattamento. Si definisce "Trattamento di dati personali" ogni elaborazione di dati (calcoli, creazione di archivi, produzione di liste e loro utilizzo) così come la semplice custodia di dati.
Ogni organizzazione mette in atto diversi Trattamenti di dati personali. Per esempio, ci sarà un Trattamento per i dati relativi ai soci, uno per i dati relativi agli assistiti, uno per i donatori. A volte la stessa persona e perfino lo stesso insieme di dati è trattato in modi diversi o per finalità diverse. Un'organizzazione, anche piccola, spesso ha da 3-4 a 8-10 Trattamenti.

Titolare. Titolare del Trattamento è l'organizzazione che ha bisogno del processo stesso e quindi l'ha ideato, promosso e lo mette in atto.
Interessato. L'Interessato è la persona alla quale appartengono i dati personali.

I documenti da preparare

Per ogni Trattamento occorre preparare una documentazione. Come minimo la documentazione consiste in:

- Informativa all'Interessato
- Modulo di consenso
- pagina nel Registro dei Trattamenti

Come minimo, perché ci sono altri moduli:
Comunicazione agli interessati, DPIA.

Nello schema vediamo i documenti creati per un'Associazione di genitori di bambini con diabete che ha un libro soci, un sito web, raccoglie donazioni, organizza degli eventi sanitari chiamati 'campi scuola' e degli eventi semplici, ha dei collaboratori professionali e tratta delle immagini.

	DPIA	Informativa	Comunicaz.	Consenso
Soci	✔	✔		✔
Mailing/Newsletter		✔	✔	✔
Campi scuola	✔	✔		✔
Eventi		✔		✔
Donazioni		✔		implicito
Immagini	✔	✔		✔
Sito		✔		✔
Professionisti	✔	✔	✔	✔

Modulo dei diritti	Registro dei Trattamenti	DPA

Informativa agli Interessati

L'Informativa descrive all'Interessato un Trattamento. In genere è lunga da due a quattro pagine. Ecco cosa contiene.

Tipologia dei dati e finalità della raccolta. Un'Informativa all'Interessato ben strutturata inizia illustrando quali tipologie di dati personali sono raccolte e perché. Occorre spiegare che si richiede all'Interessato il suo indirizzo completo per poter inviare delle lettere, il codice fiscale perché è richiesto dalla tal normativa e così via. È l'occasione per verificare se davvero tutte le informazioni richieste sono utili.

Finalità del Trattamento. Spesso illustrando le ragioni per cui sono richiesti i dati si anticipa questa informazione. Occorre spiegare perché il Titolare ha creato questo Trattamento.

Modalità del Trattamento. Seppure in modo sintetico, occorre entrare nel dettaglio e spiegare il 'viaggio' che i dati fanno all'interno dell'organizzazione vale a dire:

- come vengono raccolti (con quale forma di consenso, da chi)
- come sono custoditi (su carta, su PC o su server esterni? Se su carta come? Se su PC di chi è questo PC e dove si trova? Vengono fatti dei back up e dove? Se su server esterni, chi li possiede e dove si trovano?)
- a quali elaborazioni sono sottoposti (data base, calcoli, incroci con altri dati)
- con quali organizzazioni sono condivisi a chi sono inviati e per quale ragione.

Collocazione dei dati. Il GDPR è molto attento alla collocazione fisica dei dati. Se si trovano su un PC o su un server fisicamente collocato presso l'organizzazione (o presso l'abitazione di un socio) va tutto bene. Se sono su un server esterno o su cloud, invece, occorre sapere dove si trova quel server o quale organizzazione fornisce il servizio di cloud (Google? Amazon Web Services? Aruba?...).

Durata del Trattamento. Il GDPR è una buona occasione per 'fare pulizia'. Spesso i dati sono custoditi per tempi inutilmente lunghi. Se ci sono norme di legge che impongono una custodia lunga o indefinita occorre citarle, altrimenti meglio indicare una durata più breve possibile. La durata può essere espressa in anni o legata a un evento specifico, per esempio il compimento della maggiore età, per due anni dopo l'ultimo contatto, etc. Durate indefinite o lunghe vanno sempre giustificate.

Rischi per l'Interessato. Descritto il Trattamento, inizia la parte più strana del GDPR. Si tratta di spiegare perché l'organizzazione ritiene di avere il diritto di trattare questi dati. Siete voi a decidere, ma dovete spiegare per filo e per segno su quali basi è stata presa questa decisione.
Il primo passo è mettersi nei panni dell'Interessato e capire quale impatto potrebbe avere su di lui la cancellazione di tutti o di parte dei dati personali che detenete (generalmente l'impatto per l'Interessato, in questo caso, è limitato) piuttosto che la loro alterazione (idem) e soprattutto il rischio che questi dati siano rubati, condivisi con persone non autorizzate o diffusi. In questo ultimo caso l'impatto dipende dalla natura dei dati personali.

Misure di minimizzazione. Indicati i rischi vanno elencate, abbastanza nel dettaglio, le misure che sono state prese per ridurli. Il GDPR è un'occasione per potenziare queste misure sotto il profilo delle pro-

cedure, delle protezioni software e hardware. Ecco alcuni esempi:

- limitare il numero di persone che hanno accesso ai dati
- prevedere misure di sicurezza fisiche (spazi chiusi a chiave)
- password personali e sicure
- firewall, crittografia dei dati e altre soluzioni
- formazione degli addetti ai Trattamenti.

Legittimità del Trattamento. Il Titolare deve spiegare perché pensa di avere diritto a intraprendere o continuare questo Trattamento. La legittimità o liceità del Trattamento poggia su:

- l'interesse del Titolare (ad esempio anche raccogliere contributi è un interesse legittimo)
- la qualità dell'informazione resa all'Interessato
- la presenza di un consenso esplicito o implicito
- il fatto che i dati non sono condivisi con terzi (se non per finalità precise ed elencate).

L'Informativa si conclude con la frase di rito "Il Titolare ritiene di disporre delle basi giuridiche per mettere in opera o per proseguire il Trattamento" e con l'indicazione del nome, indirizzo postale o e-mail e telefono del Titolare, del Responsabile e del DPO.
A seguire, a titololo di esempio, una Informativa.

<Nome Associazione>
Trattamento 'soci'
Informativa agli Interessati

Categorie e Dati oggetto del Trattamento
Il Trattamento riguarda le persone che sono attualmente o sono state, in un recente passato, socie di <nome>.
I dati compresi nel Trattamento sono o possono essere:
per i minori (se esistono)
- nome, cognome;
- data e luogo di nascita;
- indirizzo

per i genitori e/o soci maggiorenni
- nome, cognome;
- data e luogo di nascita;
- indirizzo e-mail;
- numero di telefono;
- quote associative richieste/saldate

Finalità per le quali sono raccolti i dati e finalità del Trattamento
Il Trattamento 'Soci' è finalizzato alla gestione dei Libri soci dell'Associazione alla convocazione e gestione delle Assemblee dei Soci e degli organi statutari; alla corretta gestione contabile dell'Associazione e alla comunicazione con i Soci.

Modalità di Trattamento
Il Titolare inserisce i dati dei soci e i pagamenti delle quote associative nel software gestito da Responsabile del Trattamento. Il software funge da libro soci. Il Titolare custodisce indefinitamente anche i moduli di iscrizione pervenuti e i moduli di consenso.

Consenso al Trattamento
Il Trattamento riguarda solo persone che si sono fatte parte attiva nel richiedere di essere accettate come socie.
Il Titolare dispone di un consenso rilasciato dagli Interessati Interessati e ha inviato loro una Comunicazione indicando il possesso dei dati e segnalando il diritto di accesso, rettifica e cancellazione. A partire dal 25 maggio 2018 il Titolare chiederà a tutti i nuovi soci la firma di un consenso a norma del Regolamento europeo 679/2016 GDPR.

Esercizio dei diritti di accesso, modifica, cancellazione
Il Titolare si impegna ad aderire immediatamente o al massimo entro 10 giorni, alle richieste di accesso, rettifica e cancellazione dei dati personali o di opposizione a ulteriori Trattamenti qualora queste provengano dall'Interessato. Questi diritti sono accessibili anche agli Interessati minori di 18 ma maggiori di 16 anni.

Rischi per l'Interessato e misure di riduzione
In caso di perdita dei dati il danno per la privacy dell'Interessato sarebbe assai limitato. In caso di accesso indebito o di diffusione delle informazioni, il danno potrebbe essere significativo: di conseguenza <Nome Associazione> aveva già disposto e intrapreso alcune misure tese alla limitazione del rischio.
I dati non sono soggetti a ulteriori Trattamenti da parte di terzi.
I dati non sono condivisi con alcuna persona fisica o giuridica esterna al Direttivo dell'Associazione.
All'interno dell'Associazione solo il Presidente, conosce la User id e password necessaria per accedere al database Libro Soci e/o può aggiornarlo.
Il responsabile del Trattamento ha dato le più ampie garanzie in merito alla sua conoscenza del GDPR e alle misure di sicurezza software e hardware intraprese per la sicurezza dei dati trattati.
Il classificatore che contiene le copie su carta delle domande di ammissione e i consensi è custodito in un armadio chiuso a chiave presso la sede operativa dell'Associazione.
Dopo 5 anni dall'ultimo contatto con l'Interessato i dati vengono distrutti.

Legittimità e base giuridica del Trattamento dati
Considerando che:
- <Nome Associazione> non ha altra finalità che [indicare brevemente le finalità dell'Associazione]
- i dati sono necessari per la miglior esecuzione dei servizi richiesti
- i dati non saranno mai condivisi con nessuna altra Associazione o persona giuridica o fisica
- sono messe in atto da parte del Titolare procedure di sicurezza che riducono il rischio di accesso indebito o divulgazione dei dati
- sono messe in atto da parte del Responsabile del Trattamento procedure di sicurezza che riducono il rischio di accesso indebito o divulgazione dei dati
- il Titolare ha un legittimo interesse nell'organizzare i dati personali al fine di svolgere le procedure previste dalloStatuto e di comunicare con gli associati
- gli Interessati possono in ogni momento esercitare il diritto di accesso, modifica e cancellazione dei dati
- è possibile in ogni momento esercitare il diritto di accesso, modifica e cancellazione dei dati

il Titolare ritiene il Trattamento dati in questione legittimo e conforme al Regolamento europeo per la protezione dei dati personali 679/2016 e ritiene di avere la base giuridica per proseguirlo.

Titolare del Trattamento è <Nome completo dell'Associazione>

Responsabile del Trattamento <Nome completo del Responsabile>

Il Titolare, vista la natura e la scala dei dati trattati, non ritiene necessario nominare un Responsabile per la protezione dei dati (DPO).

Responsabile, DPO, DPIA

Responsabile del Trattamento è l'organizzazione che collabora con il Titolare nella gestione del Trattamento dati svolgendo un ruolo attivo e specifico. Un caso classico è lo studio che cura le paghe e contributi di un'organizzazione o il commercialista che ne segue gli aspetti contabili, o il webmaster che aiuta a gestire il sito internet. Se quel Trattamento ha uno o più Responsabili occorre citarlo con indirizzo e-mail, indirizzo postale, numero di telefono. Se non c'è si scriverà che il Titolare stesso è anche Responsabile.

DPO. Il GDPR richiede alle organizzazioni che trattano su larga scala dati 'sensibili' la nomina di un esperto esterno, il Data Protection Officer, che è pagato dall'organizzazione ma che può, anzi deve, vigilare sulla correttezza dei comportamenti dell'organizzazione stessa. Di fatto avviene abbastanza di rado che il DPO sia necessario. Se il Titolare ha un DPO deve indicarlo almeno con l'indirizzo e-mail. Altrimenti scriverà che non ce l'ha.

DPIA. Quando il Trattamento coinvolge dati personali 'sensibili' o minorenni, l'Informativa non basta. Occorre un documento più ampio chiamato DPIA. La DPIA fornisce gli stessi dati dell'Informativa ma più in dettaglio. In particolare, nella DPIA, andranno analizzati i rischi (con ragionamenti sulla probabilità e sull'impatto di un accesso indebito o di una diffusione dei dati), le misure di sicurezza e soprattutto le basi giuridiche del Trattamento. Perché è proprio necessario che l'organizzazione possieda e tratti dati così personali?

Il Consenso

In passato, a torto o a ragione, si riteneva che il perno della privacy fosse il consenso. Ora il perno è la descrizione dei processi. Il consenso è importante ma può non esserci o essere implicito, almeno per i dati trattati prima del 25 maggio 2018. Un consenso esplicito è necessario per tutti i dati raccolti dopo il 25 maggio 2018. Il consenso deve essere **informato, specifico e libero**.

Informato significa che nel modulo devono essere riportate, anche se in forma sintetica, le informazioni più importanti su:

- perché sono richiesti questi dati
- finalità del trattamento
- modalità di trattamento
- ulteriori trattamenti.

Chi sta per firmare un consenso deve sempre avere a portata di mano l'informativa. Sta a lui decidere se leggerla o meno.

Specifico significa che se il modulo è relativo a più Trattamenti, l'interessato deve poter acconsentire a un trattamento e non a un altro. Se i dati sono condivisi con terzi, l'Interessato deve dare il suo consenso specifico.

Libero significa che non è possibile subordinare all'assenso l'offerta di un servizio o di un vantaggio, sempre che questo non sia strettamente necessario o imposto da normative. Per abbonarsi a una newsletter è necessario condividere indirizzo e-mail e magari nome e cognome, ma perché devo condividere il mio codice fiscale?

Il modulo di consenso deve esplicitare la disponibilità del Titolare a consentire l'esercizio dei diritti di accesso, modifica e cancellazione dei dati e deve contenere i dati del Titolare, del Responsabile (se esiste), del Dpo (se esiste) nonché indirizzo telefonico postale e e-mail della autorità garante.
Il modulo di consenso deve essere firmato e custodito dal Titolare. È possibile prevedere un solo modulo di consenso per più Trattamenti.
Il modulo di consenso può essere separato dal modulo in cui sono scritti i dati così come può essere contestuale (dati e consensi sono forniti nello stesso modulo).

<Nome Associazione>
Modulo di consenso a norma Regolamento Europeo 679/2016 (GDPR)
SOCIO: .....

<Nome Associazione> registrerà nel Libro Soci i seguenti dati a Lei riferiti: nome, cognome, indirizzo, data di nascita, numero di telefono, codice fiscale e quote associative richieste/saldate]. Il mancato consenso a questa iscrizione rende impossibile l'iscrizione.
❑ **Acconsento al vostro trattamento di questi dati.**

<nome> desidera trattare anche l'indirizzo e-mail del socio allo scopo di inviargli comunicazioni sulle attività dell'Associazione. L'indirizzo mail sarà utilizzato per l'invio di una newsletter o per singole comunicazioni. Il consenso è facoltativo anche se fortemente consigliato.
❑ **Acconsento al vostro trattamento del mio indirizzo e-mail.** ❑ **Non acconsento**

<Nome Associazione> desidera trattare anche il numero di telefono mobile e/o fisso del socio sia per contattarlo singolarmente sia allo scopo di inviargli comunicazioni via SMS o WhatsApp sulle attività dell'Associazione. Il consenso è facoltativo anche se fortemente consigliato.
❑ **Acconsento al vostro trattamento del mio indirizzo e-mail.** ❑ **Non acconsento**

<Nome Associazione> desidera potervi inviare a casa lettere e comunicazioni sulla sua attività. Le lettere potranno indicare sulla busta il nome del mittente. Il mancato consenso rende difficile inviarVi le comunicazioni formali dell'Associazione.

❑ **Acconsento al vostro trattamento del mio indirizzo e-mail.** ❑ **Non acconsento**

<Nome Associazione> deve tenere copia cartacea di questi stessi moduli di consenso, così come del libro soci, per un periodo indefinito. Il mancato consenso a questo Trattamento rende impossibile l'iscrizione.
❑ **Acconsento al vostro trattamento di questi dati.**

Desideriamo inoltre ricordarLe che:
- ora e in qualsiasi momento può consultare o richiedere presso la nostra sede le Informative relative ai vari Trattamenti dati;
- i dati trattati non saranno condivisi con nessun'altra persona fisica o giuridica né soggetti a elaborazioni o trattamenti ulteriori;
- ci riserviamo di utilizzare il suo indirizzo di casa o mail o numero di telefono in modo moderato;
- in qualsiasi momento Lei può chiederci di sapere di quali suoi dati personali siamo in possesso, modificarli, cancellarli in tutto o in parte. Eseguiremo immediatamente le Sue istruzioni.

Data _____ nome cognome _____ firma _____

Titolare dei Trattamenti è <Nome completo dell'Associazione>

Responsabile del Trattamento <Nome completo del Responsabile>

Qualunque motivo di insoddisfazione potrà essere da Lei riportato alla Autorità Garante per la protezione dei dati personali, Piazza Venezia n. 11 - 00187 Roma, tel. 06.696771, mail garante@gpdp.it

La Comunicazione agli Interessati

In linea generale si raccoglierà il consenso esplicito e firmato per tutti i dati raccolti dopo il 25 maggio 2018 (una organizzazione potrebbe rischiare e usarlo solo per i dati raccolti dopo essersi messa a norma). Per i dati precedenti, in linea generale, si può usare un modulo di Comunicazione. Come si vede dall'esempio di seguito, il modulo di Comunicazione è simile al modulo di consenso, anche se è meno dettagliato, ma non richiede la firma. Semplicemente ricorda la disponibilità del Titolare a cessare il Trattamento qualora l'Interessato non sia d'accordo. È il meccanismo del silenzio assenso. È possibile prevedere un modulo di comunicazione per più Trattamenti.

Quando basta una Comunicazione? L'ideale sarebbe possedere un consenso per tutti i dati di cui l'organizzazione dispone. Non è strettamente necessario. Si può fare a meno del consenso quando l'Interessato è cosciente del fatto che i suoi dati sono Trattati e, indirettamente, ha acconsentito a tale Trattamento. La prova del nove è chiedersi "l'Interessato sarebbe sorpreso di sapere che possediamo questi suoi dati personali?".

Per esempio, se l'Interessato è socio o volontario dell'Associa¬zio¬ne, se ha ricevuto un servizio dall'Associazione o se ha offerto un contributo, non sarà sorpreso del fatto che l'organizzazione tratti suoi dati. In questi casi sarà sufficiente inviare una Comunicazione.

Sarà invece sorpreso se non ha mai condiviso dati con l'Associazione. In questo caso o si cancella il dato o si chiede un consenso esplicito.

<Nome Associazione>
Comunicazione agli interessati 'omnibus'

Con l'entrata in vigore della nuova normativa europea sulla privacy (Regolamento generale sulla protezione dei dati 2016/627) dobbiamo ricordarLe che,

- disponiamo dei dati necessari alla Sua iscrizione fra i Soci della nostra Associazione;
- potremmo disporre dei dati relativi ai contributi da Lei dati alla Associazione (importo, data, modalità, e a volte codice Iban, codice fiscale);
- potremmo aver utilizzato o utilizzare in futuro il Suo indirizzo mail per inviarLe messaggi dei quali custodiamo una copia;
- potremmo aver utilizzato o utilizzare in futuro il Suo indirizzo per inviarLe lettere o plichi;
- potremmo aver ricevuto o ricevere in futuro da Lei messaggi mail dei quali custodiamo una copia;
- potremmo aver inserito il suo numero di telefono in una rubrica WhatsApp o di altro sistema di messaggistica utilizzato per inviarLe messaggi individuali o diretti a interi gruppi o sottogruppi di soci;
- potremmo aver ripreso la Sua immagine in modo riconoscibile ancorché non associata ad alcun cognome e potremmo averla pubblicata sulla nostra pagina web o social media.

Visto che queste attività sono necessarie per riempire di contenuto il legame con l'Associazione di cui ha scelto di essere socio riteniamo superfluo richiedere un rinnovo del consenso implicito o esplicito da Lei prestato.

Non è necessario che Lei ci invii un consenso.

Se lo desidera può leggere alla pagina [inserire l'indirizzo della pagina web dove è stata pubblicata l'Informativa] le Informative all'Interessato dove troverà maggiori indicazioni.
Ovviamente ora e in qualsiasi momento potrà chiederci di:

- sapere quali suoi dati personali trattiamo;
- modificarli;
- cancellarli in tutto o in parte.

Eseguiremo immediatamente le Sue istruzioni.

Titolare dei Trattamenti è <Nome completo dell'Associazione>

Responsabile del Trattamento <Nome completo del Responsabile>

Qualunque motivo di insoddisfazione potrà essere da Lei riportato alla Autorità Garante per la protezione dei dati personali, Piazza Venezia n. 11 - 00187 Roma, tel. 06.696771, mail garante@gpdp.it

Il modulo dei Diritti

È una buona cosa, anche se non espressamente richiesto, produrre un modulo attraverso il quale l'Interessato può chiedere l'esercizio dei suoi diritti:

- sapere di quali dati dispone l'Organizzazione su di lui
- poterli modificare
- chiederne la cancellazione
- opporsi a ulteriori Trattamenti.

Questo modulo deve specificare – se è il caso – per quali ragioni l'organizzazione potrebbe negare questo diritto o dover sospendere un servizio se viene esercitato. In ogni caso, queste richieste vanno soddisfatte sempre al massimo entro 30 giorni se espresse in forma scritta e firmate.

Trattamenti particolari

Immagini. Le immagini fotografiche o video raccolte da una organizzazione sono dati potenzialmente sensibili, soprattutto se riguardano minori, se permettono ragionevolmente di intuire lo stato di salute o le opinioni politiche e filosofiche o religiose dell'Interessato (quando questi è, anche solo in via di ipotesi, riconoscibile). Questo è particolarmente vero se l'organizzazione intende condividere le immagini attraverso web e social media.
È sicuramente consigliabile chiedere un consenso esplicito 'anticipato' a tutte le persone che potrebbero essere ritratte (soci, volontari, assistiti) ed evitare di ritrarre persone che non lo hanno firmato. Per il passato una Comunicazione è sufficiente se il contesto è 'neutro' mentre servirebbe un consenso se non lo è.
La foto di un evento dell'Associazione Aci di Guidonia è un contesto neutro mentre un evento della Associazione Diabetici di Guidonia non lo è.
Nel caso di immagini di minori, occorre il consenso esplicito dei genitori, meglio di ambedue i genitori.

Dipendenti. Il Trattamento dei dati personali di dipendenti, stagisti e co-co-co è particolare perché, nonostante il gran numero di dati personali che il Titolare raccoglie sul dipendente e sulla sua famiglia, e nonostante la grande quantità di Titolari di ulteriore trattamento (Inps, Agenzia delle Entrate, Inail, etc.) l'interessato non può negare il suo consenso. Deve comunque essere informato.

Il Data Protection Agreement (DPA)

Agli occhi del GDPR il Titolare del Trattamento e il Responsabile del Trattamento sono sempre "complici". Per coprirsi le spalle e non avere la responsabilità di errori commessi dal Responsabile il Titolare farebbe bene quindi a stendere un accordo con il Responsabile nel quale si definisce:

- la prestazione in oggetto;
- la durata (non del contratto ma del trattamento), la natura e la finalità del trattamento;
- le tipologie di dati personali trattate;
- le categorie di persone interessate;
- gli obblighi e i diritti del cliente;
- gli obblighi e i diritti del fornitore.

Un contratto ben redatto riempie diverse pagine.

Il Registro dei Trattamenti

Ogni organizzazione deve creare e tenere aggiornato un Registro nel quale elenca tutti i Trattamenti dei dati personali. Per ciascun Trattamento occorre indicare, anche in modo molto sintetico: nome e indirizzo del Responsabile del Trattamento, di eventuali Titolari di ulteriori Trattamenti, le tipologie di dati raccolti, le modalità del Trattamento, la collocazione dei dati, la durata del Trattamento, e le modalità di raccolta del consenso. In sintesi vanno anche riportati i rischi dell'Interessato, le misure di minimizzazione dei rischi e le basi giuridiche sulle quali poggia la liceità del Trattamento.
Ogni pagina deve riportare la data di creazione del documento e degli eventuali aggiornamenti.

Nome del Trattamento: Trattamento Soci

Titolare del Trattamento	<Nome completo dell'Associazione>
Responsabile del Trattamento	<Nome completo del Responsabile>
Data Protection Officer	Il Titolare, vista la natura e la scala dei dati trattati non ritiene necessario nominare un DPO.
Categorie di Interessati	Persone fisiche che sono o sono state in passato Socie dell'Associazione
Tipologie di dati raccolti	Nome cognome, indirizzo postale, mail, telefono, data e importo di contributi e quote associative, codice fiscale, Iban, professione
Modalità di Trattamento	Informatica e Cartacea
Durata del Trattamento	Indefinita
Documenti prodotti	Informativa all'interessato Comunicazione specifica Comunicazione relativa anche ad altri Trattamenti Consenso relativo anche al Trattamento Eventi
Base giuridica	L'obbligo legale di tenere un Libro Soci di gestire la relativa contabilità, la necessità di tenere i contatti con i Soci. Le misure di riduzione del rischio approntate

Data di redazione di questa pagina del Registro _____

Il sito web

Il sito di un'Associazione è l'aspetto più visibile della sua adesione al GDPR. È consigliabile inserire nel sito una pagina dedicata alla privacy nella quale inserire tutte le informative. Questa pagina deve essere immediatamente visibile a partire da tutte le pagine del sito.
Il sito web è un Trattamento di dati personali, anzi una somma di Trattamenti. Chi si reca su un sito rilascia dati personali: in primo luogo il suo indirizzo IP che è un "numero di telefono" del PC o dello smartphone. Attraverso i cookie è possibile sapere tutto della navigazione che una persona ha fatto sul vostro sito.
Ci sono i cookie tecnici: usati per fornire un servizio migliore agli utenti. Tra questi si trovano anche i cookie che permettono a Google Analytics di funzionare. Per questi cookie non serve un consenso preventivo degli utenti ma basta menzionarli nell'Informativa.
I cookie di profilazione: servono per creare "profili utente" e permettono di inviare messaggi pubblicitari in linea con le preferenze e le scelte che emergono dalla navigazione di ciascun utente. Qui servirebbe un consenso preventivo e comunque un'Informativa su quali cookie di profilazione sono utilizzati. Poi ci sono i cookie utilizzati all'interno del vostro sito ma che provengono da terze parti.
Da ultimo ci sono i dati raccolti attraverso dei moduli on line. Se possibile è meglio evitarli. Altrimenti anche loro richiedono una documentazione: informativa, consenso e comunicazione.

Riassunto: cosa, dove, come, quando

Una volta definita la documentazione occorre disporre i moduli nel modo corretto.

Vanno tenuti in una copia presso la sede dell'Associazione: il Registro dei Trattamenti, eventuali DPIA, eventuali DPA, un faldone con tutti i moduli di consenso firmati e, in più copie, il Modulo dei Diritti e tutte le Informative.

Vanno duplicati in più copie e resi disponibili nel luogo in cui sono raccolti i dati: Moduli di Consenso e Informative all'Interessato.

È essenziale che gli interessati possano disporre dell'Informativa nel momento in cui leggono il Modulo di Consenso o la Comunicazione. Occorre quindi farne diverse copie e metterle on line.

Le Comunicazioni vanno inviate agli Interessati.

E dopo?
Formazione e aggiornamento

La formazione degli addetti al Trattamento cioè di tutte le persone che, a qualsiasi titolo, possono avere accesso ai dati personali è un aspetto centrale del GDPR.
L'ideale sarebbe organizzare un corso interno ma di rado è possibile.
Il "minimo sindacale" consiste probabilmente nel chiedere a ciascuna persona di leggere la documentazione relativa al Trattamento o ai Trattamenti ai quali potrebbe prendere parte. Per documentare l'avvenuta lettura si può chiedere a ogni persona di siglare per presa visione ogni pagina. Lo stesso potrebbe avvenire almeno per alcune pagine di questo libretto.
Il GDPR non è un atto ma un processo. È necessario prevedere una documentazione ad hoc per ogni nuovo Trattamento di dati personali (ad esempio a seguito di una nuova iniziativa).
È importante anche, almeno una volta all'anno, rileggere tutta la documentazione per vedere se qualche cambiamento nella attività della Associazione o nella normativa ha reso necessaria una modifica della documentazione stessa.

CSV - Centro di Servizio
per il Volontariato del Lazio
Via Liberiana, 17 - 00185 Roma
tel. 06.491340 (CESV)
email: info@cesv.org