

Oggetto: Regolamento Europeo sulla privacy (GDPR) – parere alle Associazioni della FAP

È stato emanato il nuovo Regolamento Europeo in tema di privacy, il c.d. GDPR (*General data protection regulation*), entrato in vigore il 25 maggio 2018.

Più specificamente, si tratta del “*REGOLAMENTO (UE) DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 N. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati – GDPR, General data protection regulation)*”.

L’ Italia non ha ancora emanato alcun Decreto relativo, ma il Regolamento è già pienamente in vigore poiché si tratta infatti di un Regolamento Europeo “*auto-applicativo*”, mentre il Decreto nazionale deve servire solo ad aggiornare le norme interne obsolete.

Il Regolamento Europeo è stato emanato tenendo ben presente la grave problematica di colossi del web come Google e Facebook, e quindi si tratta di un regolamento molto rigoroso, con pesanti sanzioni.

Il GDPR mira a responsabilizzare pienamente chiunque esegua un trattamento di dati personali altrui, e mira a tutelare adeguatamente tutti gli interessati a cui si riferiscono i dati personali.

Si tratta di materia assai vasta e complessa, su cui sono stati pubblicati grossi volumi. Qui ci concentreremo sulle esigenze pratiche delle Associazioni della FAP nei confronti dei loro iscritti.

Anticipiamo subito che per i dati personali raccolti prima del 25 maggio 2018 (data di entrata in vigore del nuovo Regolamento Europeo:

- una nuova dichiarazione di consenso dell’iscritto non è necessaria;
- una nuova informativa da parte dell’ associazione nei confronti dell’ iscritto è quanto-meno opportuna e generalmente è anche necessaria.

1. I principi generali del GDPR

Il principio fondamentale del GDPR è quello secondo cui, al di fuori dell’ambito personale e domestico, non è consentito detenere dei dati personali altrui senza che vi sia un valido motivo, che non può essere la mera utilità personale di chi li detiene, oppure delle finalità che non siano chiare e trasparenti.

Ogni trattamento dei dati deve essere lecito e giustificato, altrimenti si considera vietato. Così si esprime in sintesi la norma:

Art. 5 del GDPR

Principi applicabili al trattamento di dati personali

1. I dati personali sono:

- A) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; [...] («**limitazione della finalità**»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);
- d) esatti e, se necessario, aggiornati; [...] («**esattezza**»);
- e) [...] per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; [...] («**limitazione della conservazione**»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali [...] («**integrità e riservatezza**»).

2. La liceità del trattamento dei dati personali

Il trattamento dei dati personali deve essere lecito e giustificato da una “base giuridica”, quindi da un valido motivo, che essenzialmente può essere:

- 1. Il mero consenso dell'interessato per una specifica finalità; oppure alternativamente
- 2. L'esecuzione di un contratto (o di altro obbligo legale).

Così infatti si esprime in sintesi l'art. 6 del GDPR:

ARTICOLO N.6

Liceità del trattamento

- 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
 - a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
 - b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato [...];
 - c) [...] *Seguono molte altre ipotesi che qui non rilevano.*

La base giuridica “congiunta” del trattamento dei dati

Qualche volta la “base giuridica” del trattamento dei dati può essere costituita congiuntamente da entrambe le ipotesi.

Ad esempio un avvocato può ricevere un mandato da un cliente, e allora i dati personali gli servono per avviare la causa, in esecuzione del contratto di patrocinio. In questo caso l'avvocato fornirà la informativa sul trattamento dei dati, e se il cliente gli conferirà l'incarico difensivo accetterà il suddetto trattamento dei dati perché questo è finalizzato alla gestione della causa.

In questo caso non occorrerà una seconda dichiarazione di consenso del cliente, poiché il conferimento del mandato (ovvero la stipulazione del contratto) comprende già l'accettazione del trattamento dei dati necessari.

I dati però sono conferiti per questa sola finalità, e quindi l'avvocato non potrà ad esempio comunicare ad aziende gli elenchi dei clienti o dei pazienti a scopo commerciale o pubblicitario.

Ipotizziamo però che il cliente voglia anche essere inserito nella mailing list dello Studio, per tenersi aggiornato su alcune problematiche. Questo è un fatto ulteriore rispetto all'avvio di una causa, e potrebbe non essere compreso nell'incarico professionale conferito con il mandato difensivo.

In questo caso il cliente dovrà dare il suo consenso a tale invio della newsletter.

In conclusione in queste ipotesi il diritto dell'Avvocato al trattamento dei dati del cliente avrà un duplice fondamento:

- Nel contratto di patrocinio per quanto riguarda i dati necessari a gestire la causa;
- Nel consenso del cliente per le ulteriori finalità (come la newsletter) che non sono strettamente necessarie per la gestione della causa.

Il caso pratico dell'Associazione

Se trasferiamo questa problematica nei rapporti fra l'Associazione ed i suoi iscritti, dobbiamo concludere in modo analogo.

- L'iscritto all'atto della iscrizione (o con il suo rinnovo) stipula un contratto di associazione, aderendo ad uno statuto che indica le finalità dell'Associazione. I suoi dati necessari per la tutela dei suoi interessi, conferiti secondo le finalità associative (che possono essere anche molto ampie), sono liberamente trattabili dall'Associazione, senza alcuna necessità di ulteriore e separata dichiarazione di consenso. La base giuridica del trattamento dei dati sarà l'esecuzione del contratto associativo, ai sensi della lettera b) dell'art. 6.

I dati personali risultano necessari per l'adesione all'associazione, sia per la verifica degli eventuali requisiti per l'iscrizione e sia per il raggiungimento degli scopi statutari dell'associazione, ovvero la tutela dei suoi iscritti.

- L'Associazione potrebbe inoltre voler trattare i dati personali per finalità ulteriori rispetto a quelle previste dallo Statuto associativo. In questo caso è necessario il separato consenso dell'iscritto e la base giuridica del trattamento dei dati è costituita dal "consenso" di cui alla lettera a) dell'art. 6.

In conclusione:

- Se l'iscritto non ha mai firmato alcuna dichiarazione di consenso separato al tratta-

mento dei dati, sarà comunque possibile trattare i suoi dati necessari per le finalità associative (e quindi per esempio inviargli i notiziari e le comunicazioni)

- Se l'iscritto al contrario, ha firmato all'atto della iscrizione (o successivamente), magari nello stesso testo firmato per l'iscrizione, anche il consenso all'ulteriore trattamento dei dati per finalità ulteriori rispetto allo Statuto, sarà possibile utilizzare questa sua dichiarazione per tali finalità.

Vi allego l'apposito modulo da utilizzare preferibilmente in futuro all'atto dell'iscrizione o del suo rinnovo.

Approfondimento: la normativa dettagliata sul consenso per una finalità specifica

Il GDPR così si esprime nella premessa al testo del Regolamento (il c.d. "Considerando" al n. 32)

"(32) Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. [...].

Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle.

Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità.

Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

Aggiunge il GDPR, all'art. 7, comma 2, che:

"2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.[...]."

In concreto occorrerà:

- Scrivere in modo molto chiaro la dichiarazione, evidenziando le finalità (in modo ampio);
- Separare il testo del consenso dal testo relativo all'iscrizione;
- Non vi devono essere caselle di testo pre – spuntate, o approvate in modo implicito o presunto.

Aggiungiamo ancora che se la finalità cambia rispetto a quella originaria, occorrerà allora comunicare questo all'interessato e richiedere un nuovo consenso.

3. Il divieto di trattamento dei dati per motivi diversi da quelli associativi

Naturalmente l'associazione che riceve (legittimamente) i dati personali rimane vincolata a non usare questi dati per scopi diversi da quelli associativi, e quindi non potrà trasmetterli a soggetti estranei al raggiungimento degli scopi associativi.

Invece rientrano nei possibili destinatari dei dati suddetti quegli ausiliari (ad es. i professionisti)

cui l'associazione si rivolge per il raggiungimento degli scopi associativi. Quindi ad esempio l'associazione potrà fornire i dati ad un consulente legale o ad un attuario, ma non ad aziende terze per finalità meramente commerciali.

In questi casi sarebbe bene comunicare agli interessati che i dati potrebbero essere forniti ad altre associazioni similari o alla FAP, nell'ambito degli stessi scopi di tutela degli iscritti.

Per le modalità di comunicazione di tale informativa, si veda più avanti.

4. il dovere di informativa agli interessati

Abbiamo visto che chi aderisce all'associazione non deve necessariamente aggiungere una ulteriore dichiarazione di consenso, essendo tale consenso già compreso nella sua iscrizione (o nel suo rinnovo).

Va però ribadito che l'associazione deve comunque fornire agli interessati una adeguata informativa, come tutti i soggetti che trattano i dati personali altrui.

Le norme essenziali del GDPR in proposito sono le seguenti:

Art. 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. [...].

Il contenuto dell'informazione è regolato minutamente dal GDPR all'art. 13, ed è quindi necessario che chi raccoglie i dati fornisca una adeguata informativa all'interessato su alcuni aspetti:

1. Motivo per cui dati vengono richiesti;
2. Titolare dei dati suddetti e suoi recapiti;
3. Responsabile del trattamento dei dati;
4. Diritti dell'interessato su questi dati (accesso, modifica, aggiornamento, cancellazione, durata del trattamento, ecc.).

Art.13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
 - c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
 - d) [...];
 - e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
 - f) [...]
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
 - c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
 - d) il diritto di proporre reclamo a un'autorità di controllo;
 - 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;
 - f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

A seguito di questa informativa, l'interessato potrà esercitare i suoi diritti, che elencati più avanti.

5. I dati personali raccolti prima del 25 maggio 2018

Per i dati raccolti prima del 25 maggio 2018 (data di entrata in vigore del nuovo regolamento europeo) non è necessaria una nuova dichiarazione di consenso dell'iscritto, perché aveva già aderito all'associazione.

Altro discorso è quello del dovere di informativa all'interessato, tenuto conto della necessità che il titolare del trattamento fornisca una adeguata informativa sulle modalità e finalità del trattamento stesso.

In linea teorica il titolare del trattamento può essere esonerato da quest'obbligo se ha in precedenza fornito un'adeguata informativa. In concreto però le informative fornite in base alla precedente normativa difficilmente contenevano tutti gli elementi che oggi vengono richiesti dal nuovo regolamento.

Quindi è quanto meno opportuno, se non doveroso, fornire a tutti gli interessati a questa nuova informativa.

La forma di questa informativa, secondo il GDPR, non è necessariamente scritta, e teoricamente potrebbe addirittura essere fornita in forma orale. Resta però la fondamentale esigenza che il titolare del trattamento debba poter provare di aver fornito questa informativa, ed allora quindi la forma scritta diventa veramente opportuna.

In concreto è bene inviare tale informativa anche in forma di e-mail laddove possibile, ed altrimenti in forma cartacea per chi è sfornito di e-mail, aggiungendo che è opportuno poter conservare una forma di riscontro dell'interessato.

6. Il sito dell'Associazione

E' veramente opportuno, inoltre, fornire questa informativa agli iscritti sul trattamento dei dati anche tramite il sito dell'associazione, e quindi è bene aggiungere nell' informativa scritta agli iscritti anche il link alla apposita pagina del sito.

Va evidenziato in proposito che il sito dell' Associazione può sempre essere opportuno aggiornato, evitando di dover fornire nuove informative ai singoli iscritti.

Inoltre il sito dovrà fornire due altre informative:

1. **i cookie:** si tratta di una questione molto tecnica, ma in sostanza è sufficiente illustrare in un'apposita pagina questa problematica e chiedere un semplice click. In internet sono reperibili alcuni testi accurati di quest' informativa tecnica. Non è necessario che l' associazione spenda soldi in tecnici informatici.

Ve ne giro una che mi sembra valida anche sotto il profilo informatico (e voi sapete che su questo ho qualche competenza, poiché sabato 14 luglio ultimerò il corso che sto seguendo per gestire i siti in WordPress, con un relativo attestato di cui vado molto orgoglioso).

2. **La privacy:** la gestione dei dati personali da parte dell'Associazione, compresi quelli acquisiti tramite il sito (tramite moduli, form o registrazioni).

E' indispensabile che il Presidente dell'Associazione, in quanto titolare dei dati personali, conservi personalmente le credenziali sempre aggiornate del sito, ovvero le password da amministratore del sito, comprese quelle sulla gestione del dominio presso l' *host*.

Nessun altro soggetto può sostituirsi in questo ruolo al Presidente.

7. I vari soggetti indicati dal GDPR

Il GDPR indica una articolata serie di definizione dei soggetti indicati.

Per semplificare abbiamo così sintetizzato la norma di cui all' art. 4:

Art. 4 - Definizioni

Ai fini del presente regolamento s'intende per:

- 1) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);[...]
- 2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali [...];
- 3) [...];
- 7) **«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; [...];
- 8) **«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;
- 9) **«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. [...];

In pratica:

1. Il **«titolare del trattamento»** (**“Data Controller”**) sarà l' Associazione, in persona del suo Presidente. Richiamiamo quanto già scritto dal compianto Stefano Rodotà nel suo provvedimento in materia emanato dal Garante per la protezione dei dati personali il 9 dicembre 1997: *“In altre parole, qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il “titolare” è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)”*.

Aggiungiamo ancora che la parola inglese **“Data Controller”** è infelicemente tradotta in italiano con **“titolare del trattamento”**. Titolare ha, nella lingua italiana, un significato evocativo che può trarre in inganno; il *Data Controller* non è infatti titolare, padrone, dei dati, ma solamente *del trattamento dei dati*, i quali restano però di esclusiva 'proprietà' del soggetto a cui si riferiscono, che in termini *privacy* si definisce l'**interessato** (in inglese è il **Data Subject**). La caratteristica fondamentale del titolare è la capacità di **“determinare finalità e mezzi del trattamento”** (art. 4 del Gdpr).

2. Il **«responsabile del trattamento»** sarà colui tratta i dati per conto del titolare, ovvero sotto le concrete direttive del Presidente, il quale esprime la volontà dell' Associazione. Il **“responsabile del trattamento”** corrisponde all' inglese **“Data Processor”**, che è stato tradotto in italiano in modo fuorviante: quello che si vuole definire è **“la persona fisica**

o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare" (art. 4 del GDPR). Il responsabile quindi entra in gioco quando il titolare decide di delegare parte del trattamento ad un soggetto esterno e può quindi essere definito come la *longa manus* del titolare: esso è privo di autonomia nel decidere come e per quali ragioni può trattare i dati degli interessati.

3. Gli **"addetti al trattamento"** saranno coloro che collaborano per il trattamento dei dati, sotto la direzione del Presidente. Sono previsti dall' art. 29: "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento. Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento.

8. Il responsabile della protezione dei dati

Il GDPR prevede anche la figura *eventuale* del **responsabile della protezione dei dati** (in lingua inglese **data protection officer – DPO**).

Si tratta di una figura che non interessa affatto le associazioni (si vedano in proposito i chiarimenti del Garante al seguente [link](#)), poiché è prevista dall' art. 37 per le grandi aziende o per gli enti pubblici.

Purtroppo mi è capitato di sentire ultimamente di qualche soggetto che ha cercato di assumere tale carica inutile e costosa, magari senza avere neppure le necessarie qualità professionali, che nell' art. 37 sono così descritte:

"5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi".

Questo soggetto non va assolutamente confuso con il "**responsabile del trattamento**", ed è un consulente qualificato che serve a fornire consulenza ai "**titolari del trattamento dei dati**", ma senza per questo esonerarlo da alcuna responsabilità. Deve trattarsi di un professionista molto qualificato (avvocato specializzato in materia o ingegnere informatico con specifica esperienza di protezione dei dati) ed il suo nominativo va comunicato al Garante della privacy. Si tratta quindi di un costo inutile e chiaramente spropositato per le limitate finalità di un'associazione.

9. Il problema della sicurezza e della riservatezza dei dati

Un altro obbligo che ha il titolare dei dati è quello di curare la loro sicurezza, impedendo che siano accessibili a terzi non autorizzati.

E' bene quindi che i dati conservati in un computer siano protetti da password, e i dati custoditi in forma cartacea siano adeguatamente protetti dall'accesso di soggetti non autorizzati.

Il Presidente dell'Associazione dovrà disporre costantemente di tutte le password aggiornate di

qualsiasi archivio di iscritti, degli indirizzi di posta elettronica usata, nonché del sito dell'associazione. Tale esigenza è inderogabile.

10. I dati sensibili

Un discorso ulteriore va fatto per i cosiddetti dati sensibili, che sono definiti nell'articolo 9, che così li elenca:

Art. 9 - Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, [...]

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

[...]

In pratica è possibile trattare questi dati sensibili in due ipotesi essenziali:

1. Il consenso specifico per finalità specifiche;

2. Il trattamento è effettuato da parte di un'Associazione che persegue finalità sindacali, purché il trattamento riguardi unicamente i suoi membri, gli ex membri o le persone che hanno regolari contatti con [...] l'associazione.

È quindi opportuno che le associazioni curino in modo particolare l'acquisizione del consenso da parte dei congiunti degli iscritti, nell'ipotesi che vengano acquisiti i loro dati sensibili, come quelli in materia di salute, soprattutto per quanto riguarda le associazioni che gestiscono polizze sanitarie.

Sarà quindi necessario acquisire lo specifico consenso dei congiunti dell'iscritto interessati a queste polizze, sia all'atto della sottoscrizione e sia all'atto al momento dei successivi si rimborsi.

11. I diritti degli interessati

Per "interessati" ("Data Subject") si intendono i soggetti cui i dati personali si riferiscono.

Purtroppo la traduzione italiana della terminologia europea è stata molto infelice.

Nel testo italiano si parla di "interessati" per indicare in realtà i veri "titolari" dei dati, e quindi

ad esempio deve essere chiaro il vero titolare dei miei dati personali sono ovviamente solo io.

Chi è autorizzato a trattare i miei dati, è solo il “titolare del trattamento”, ma ovviamente il titolare dei miei dati resto solo io, che però vengo definito nel GDPR in italiano solo “interessato”.

Secondo il GDPR i diritti dell’ interessato sono essenzialmente questi:

Art. 15 - Diritto di accesso dell'interessato

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. [...].

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. [...].

12. Conclusioni operative per le Associazioni

In concreto, per quanto riguarda le Associazioni, la situazione sarà la seguente.

1. Non occorrerà richiedere un nuovo consenso degli iscritti, tenendo però presente la necessità di consenso dei congiunti per i dati sensibili, nonché da parte di ogni interessato per ogni singolo rimborso per le polizze sanitarie;
2. Occorrerà fornire a ciascun iscritto l’informativa di cui al modulo che allego;
3. Occorrerà comunicare nell’ informativa all’ iscritto i dati del titolare (Associazione e suo Presidente, che dovrebbe essere nominativamente indicato con i suoi recapiti), nonché del Responsabile del trattamento dei dati, con i suoi recapiti;
4. Sul sito dell’Associazione andranno pubblicati:
 - a. I dati ed i contatti dell’Associazione e del suo Presidente;

- b. I dati ed i contatti del Responsabile del trattamento dei dati
 - c. L' informativa sulla privacy
 - d. L' informativa sui cookies
5. Il Presidente deve disporre di tutte le password dell'Associazione, ivi comprese quelle del sito (dominio e *host*), degli archivi informatici, degli indirizzi mail, dei *clouds* (come Drop-box) e dei servizi di raccolta dati (Jotform e simili);
 6. Non occorre invece la figura del DPO, ovvero del responsabile della protezione dei dati.
 7. Occorre inoltre vietare che sorgenti soggetti diversi dal titolare e dal responsabile del trattamento (oltre ai loro ausiliari) possano accedere ai dati degli iscritti. In particolare va escluso che la banca dati possa essere nella titolarità di tecnici informatici o altro, che gestiscono solo la manutenzione del software;
 8. Non pare strettamente necessario, al momento, il Registro del trattamento dei dati, ma su questo fornirò in prosieguo ulteriori chiarimenti, anche in base all' emanando Decreto e alle future istruzioni del Garante.

Ho cercato di fornire essenzialmente delle istruzioni operative e di utilità pratica.

La materia è vasta e complessa, ed ancora non è completato il quadro normativo.

Nel dubbio, è naturalmente meglio tenersi prudenti.

Resto a disposizione e porgo i miei migliori saluti.

Avv. Michele IACOVIELLO

Allegati:

1. Informativa da parte dell' Associazione agli iscritti
2. Informativa sui cookie da pubblicare sul sito
3. Dichiarazione di consenso dell' iscritto