12 novembre 2018

La privacy e il GDPR nelle Associazioni Sportive Dilettantistiche

A cura di Alessio Scaglia.

Il trattamento dei dati personali è un tema che investe in modo trasversale la vita di tutte le persone e coinvolge, chiaramente, anche le Associazioni Sportive Dilettantistiche.
Questi Enti, infatti, si trovano a gestire una molteplicità di dati (personali e anche sanitari) relativi ai propri associati, collaboratori, dipendenti e via discorrendo.
La c.d. *privacy* fino al **24 maggio 2018** era disciplinata dal famoso d. lgs. 196/03.
A decorrere dal 25 maggio 2018, la materia è disciplinata da una fonte normativa sovrannazionale che è il Regolamento 27 aprile 2016 n. 2016/679/UE, altrimenti noto come GDPR (il cui acronimo significa: **General Data Protection Regulation**) o, per volerlo leggere in italiano, RGPD (il cui acronico significa: Regolamento Generale sulla Protezione dei Dati Personali).
Il GDPR è un regolamento che trova diretta e immediata applicazione in tutti gli Stati dell'Unione Europea e, quindi, anche in Italia.
Inoltre, dal mese di agosto 2018, la materia della privacy è disciplinata anche dal **d. lgs. 196/03, come modificato dal d. lgs. 101/2018**.

Nel nuovo contesto normativo ci sono princìpi che informano l'intera materia:

- ***Accountability***: questo termine è difficilmente traducibile in italiano: nel contesto del GDPR assume il significato di responsabilizzare il titolare del trattamento dei dati personali indirizzandolo ad adottare tutte le misure necessarie affinché i dati trattati siano protetti e, al contempo, gli impone di rendere conto (in caso di controllo, all'Autorità competente) in merito alle misure adottate;
- ***Privacy by default* e *privacy by design***: la protezione dei dati personali deve essere l'impostazione **predefinita** all'interno di un processo di trattamento dei dati personali (*privacy by default*) che deve avvenire sin dall'inizio della progettazione delle misure tecniche idonee a garantire la sicurezza dei dati.

Vi sono, poi, tre aspetti che assumono una rilevanza fondamentale:

- **la responsabilità nel trattamento dati**: individuazione del responsabile del trattamento e raccolta e gestione di dati che siano strettamente necessari allo svolgimento dell'incarico;
- **i limiti all'utilizzo dei dati**: modalità e tempi di utilizzo e conservazione dei dati;
- **i diritti del cittadino al corretto trattamento**: in modo particolare, è previsto che il titolare del trattamento comunichi in modo chiaro e preciso come avviene il trattamento e quali diritti sono previsti in favore dell'interessato.

Le definizioni e i princìpi generali del GDPR.
In primo luogo, si evidenzia che la nuova disciplina contenuta nel Regolamento europeo si applica al **trattamento** dei dati personali delle **persone fisiche**. Il GDPR non offre alcuna tutela, invece, alla protezione dei dati personali delle persone giuridiche (come peraltro, già avveniva sotto la vigenza del d. lgs. 196/03 nella sua vecchia formulazione).
Il Regolamento fornisce una serie di definizioni che sono di fondamentale importanza per capire l'ambito applicativo della disciplina. Di seguito si riportano le definizioni più rilevanti.

Sono considerati **dati personali** tutte le informazioni che riguardano una persona fisica identificata o identificabile, la quale è definita "**interessata al trattamento dei dati personali**".

Il **trattamento dei dati personali**, invece, è definito come "*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***".

Altre due definizioni molto importanti sono quelle di titolare e responsabile del trattamento.

Il primo è definito come la persona fisica o giuridica che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**. Il responsabile del trattamento, invece, è la persona fisica o giuridica che **tratta** dati personali per conto del titolare del trattamento.

Per quanto concerne le Associazioni Sportive Dilettantistiche, esse sono soggette all'applicazione del GDPR in quanto trattano dati personali di persone fisiche; esse, invece, non soggiacciono ad alcun obbligo previsto dal GDPR quando trattano dati personali di soggetti diversi dalle persone fisiche; allo stesso modo, quando l'Associazione Sportiva opera come interessata al trattamento dei dati perché, per esempio, fornisce i propri dati ad un soggetto che li dovrà trattare, non gode delle tutele previste dal GDPR.

ESEMPIO:

L'Associazione Sportiva Beta, nata nel mese di ottobre 2018, riceve l'iscrizione di 12 atleti; prima ancora di raccogliere i dati degli atleti, l'Associazione Sportiva deve rilasciare l'informativa privacy e ottenere il consenso al trattamento dei dati da parte di ciascun atleta interessato.

La medesima Associazione, dovendo organizzare i corsi e gli allenamenti, instaura una collaborazione con un istruttore sportivo. Anche in questo caso, il primo adempimento da fare è quello di rilasciare un'informativa privacy e ottenere il consenso al trattamento dei dati personali.

L'Associazione, inoltre, stipula con Gamma S.r.l. un contratto di locazione avente ad oggetto l'immobile (di proprietà di Gamma S.r.l.) dove l'Associazione Sportiva Dilettantistica Beta andrà a svolgere la propria attività.

Ebbene, in relazione a questo contratto, l'Associazione Sportiva e Gamma S.r.l. non hanno (reciprocamente) alcun diritto di ricevere l'informativa sul trattamento dei dati personali né è necessario che prestino il proprio consenso l'un l'altra per il trattamento dei dati in forza del GDPR: questo perché, come detto, tale normativa si applica solo alle persone fisiche.

Tuttavia, potrebbe essere necessario rilasciare l'informativa e ottenere il consenso al trattamento dei dati personali da parte dei rispettivi legali rappresentati delle due distinte parti del contratto, in quanto costoro sono persone fisiche e ciascuna parte (locatrice e conduttrice) tratterà i dati del legale rappresentante dell'altra.

Per quanto riguarda i princìpi fondamentali, la norma di riferimento è contenuta nell'art. 5 del Regolamento il quale prevede che i dati personali debbano essere:

- trattati in modo **lecito**, **corretto** e **trasparente** nei confronti dell'interessato: c.d. **principio di liceità, correttezza e trasparenza**;
- raccolti per **finalità determinate**, **esplicite** e **legittime**: c.d. **principio della limitazione della finalità**;
- **adeguati**, **pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati: c.d. **principio della minimizzazione dei dati**;
- **esatti** e, se necessario, **aggiornati**: c.d. **principio di esattezza**;

- **conservati** in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati: c.d. **principio di limitazione della conservazione**;
- trattati in maniera da garantire un'adeguata **sicurezza** dei dati personali: c.d. **principio dell'integrità e riservatezza**.

Circoscrivendo l'attenzione alle Associazioni Sportive Dilettantistiche, ai sensi dell'art. 6 del Regolamento, il trattamento dei dati personali è da considerarsi lecito qualora ricorra almeno una delle seguenti ipotesi:

- il trattamento è effettuato sulla base di un **consenso** prestato dall'interessato;
- il trattamento è necessario **all'esecuzione di un contratto** del quale è parte l'interessato;
- il trattamento è necessario per **adempiere un obbligo legale** al quale è soggetto il titolare del trattamento.

ESEMPIO:
L'Associazione Sportiva Dilettantistica Beta ha rilasciato ai propri atleti l'informativa e ha ottenuto, da parte di costoro, il consenso al trattamento. A questo punto, l'Associazione è legittimata ad effettuare tutte le operazioni che danno luogo al trattamento dei dati di ciascun atleta.
L'Associazione Sportiva Beta, inoltre, ha stipulato un contratto di collaborazione con un istruttore. In questo caso, anche se non vi è un esplicito consenso dell'interessato, il trattamento è lecito per dare esecuzione al contratto.
L'Associazione Sportiva Dilettantistica Beta subisce un controllo da parte dell'Agenzia delle Entrate in merito alla sussistenza dei requisiti *ex* legge 398/1991. Nella fase di accertamento, l'Amministrazione Finanziaria chiede di poter visionare il libro soci (nel quale, evidentemente, sono contenuti i dati di tutti gli associati). Anche in questo caso, qualora ciascun interessato non avesse prestato il proprio consenso, il trattamento (cioè la comunicazione dei dati personali degli associati all'Amministrazione Finanziaria) è da considerarsi lecito in quanto effettuato in forza di un obbligo legale.

Il consenso al trattamento.
L'art. 7 del Regolamento prevede che, nel caso in cui il trattamento sia fondato sul consenso, il titolare del trattamento deve poter dare prova che l'interessato abbia dato il proprio assenso al trattamento dei dati personali.
Il consenso reso in forma scritta deve essere **comprensibile**, **facilmente accessibile** e con un **linguaggio semplice e chiaro**. L'interessato ha sempre il diritto di **revocare il proprio consenso** in qualsiasi momento, ma ciò non può pregiudicare il trattamento precedentemente effettuato in virtù del consenso prestato.

Il trattamento di categorie particolari di dati personali.
L'art. 9 del Regolamento stabilisce, in termini assolutamente perentori, il divieto di 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*".
Sono previste, tuttavia, delle deroghe. Infatti, il trattamento di questi dati (per quanto riguarda la Associazioni Sportive Dilettantistiche, dati che possono rivelare l'originale razziale o etnica o dati relativi alla salute) può avvenire **in forza del consenso prestato dall'interessato** che, in questo caso, deve necessariamente essere **esplicito** e rivolto ad una o più attività specifiche.

Il trattamento dei dati personali effettuato dalle Associazioni Sportive Dilettantistiche in forza delle Autorizzazioni del Garante per la protezione dei dati personali nn. 2 e 3 del 15 dicembre 2016.

Prima dell'entrata in vigore del GDPR, il Garante della Privacy ha emanato l'Autorizzazione Generale n. 3/2016 con la quale **ha autorizzato le associazioni** (anche non riconosciute) al trattamento dei **dati sensibili** (i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale).
L'autorizzazione è rilasciata per **il perseguimento di scopi determinati e legittimi individuati dalla legge, dall'atto costitutivo, dallo statuto** o dal contratto collettivo, ove esistenti, e in particolare per il perseguimento di finalità culturali, religiose, politiche, sindacali, **sportive o agonistiche di tipo non professionistico**, di istruzione anche con riguardo alla libertà di scelta dell´insegnamento religioso, di formazione, di ricerca scientifica, di patrocinio, di tutela dell'ambiente e delle cose d´interesse artistico e storico, di salvaguardia dei diritti civili, nonché di beneficenza, assistenza sociale o socio-sanitaria.
Con l'autorizzazione n. 2/2016, invece, il Garante ha autorizzato le associazioni e agli altri organismi che gestiscono impianti o strutture sportive, limitatamente ai dati idonei a rivelare lo stato di salute e alle operazioni indispensabili per accertare l'idoneità fisica alla partecipazione ad attività sportive o agonistiche.
Con l'entrata in vigore del GDPR (avvenuta in data 25 maggio 2018), si è posto il problema della valenza delle predette autorizzazioni.
Il Garante per la protezione dei dati personali, con proprio provvedimento del 19 luglio 2018, ha stabilito che in attesa del coordinamento tra normativa nazionale e normativa europea, "*le Autorizzazioni generali, adottate in data 15 dicembre 2016 (con Provvedimenti pubblicati sulla Gazzetta Ufficiale n. 303 del 29 dicembre 2016), per taluni trattamenti di categorie* ***particolari di dati personali*** *e di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza,* ***si intendano in vigore fino all'adozione di eventuali misure che potranno essere previste nel decreto legislativo di adeguamento della disciplina in materia****, riservandosi ulteriori valutazioni all'esito del predetto percorso normativo*".
Successivamente il Governo ha approvato un decreto legislativo che ha lo scopo di coordinare la normativa nazionale con quella europea. L'art. 22, comma 4 d. lgs. 101/2018 prevede espressamente che "***A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto***".
Ad oggi, pertanto, il trattamento dei dati personali (compresi quelli relativi alla salute) effettuato dalle Associazioni sportive dilettantistiche è da considerarsi lecito, a prescindere dal consenso ricevuto dall'interessato, in forza delle citate Autorizzazioni Generali del Garante Privacy.

L'informativa sul trattamento dei dati personali.
L'art. 13 del Regolamento disciplina il contenuto dell'informativa che deve essere resa all'interessato in relazione al trattamento dei suoi dati personali.
La norma impone al titolare del trattamento di rilasciare all'interessato, nel momento in cui sono ottenuti i dati, un'informativa con i seguenti contenuti (si indicano solamente i requisiti che rilevano per le Associazioni Sportive Dilettanstiche):

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) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

e) l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
f) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
g) 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;
h) se il trattamento è fondato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
i) il diritto di proporre reclamo a un'autorità di controllo;
j) 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;
k) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

A prescindere dalla base giuridica del trattamento, è assolutamente necessario fornire all'interessato l'informativa relativa al trattamento dei dati personali. Se il trattamento è effettuato in forza delle autorizzazioni generali, si dovrà indicare tale circostanza nel campo dedicato alla base giuridica del trattamento.

Il registro del trattamento.

L'art. 30 del GDPR ha istituto l'obbligo, per determinati soggetti e in presenza di determinate condizioni, di istituire il **registro delle attività di trattamento dei dati personali**.

Si tratta di uno strumento di *compliance* che serve al titolare del trattamento (e al responsabile del trattamento ove nominato) di individuare le misure di sicurezza adottate per la protezione dei dati personali e, al contempo, di garantire all'Autorità di controllo una puntuale verifica sulle attività svolte.

Il registro può essere tenuto sia in formato elettronico sia in formato cartaceo e deve essere esibito all'Autorità di controllo qualora vengano effettuate delle verifiche.

Secondo la disposizione dell'art 30 GDPR, il registro deve contenere le seguenti informazioni:

a) il **nome e i dati di contatto del titolare del trattamento** e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le **finalità** del trattamento;
c) una descrizione delle **categorie di interessati e delle categorie di dati personali**;
d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i **destinatari di paesi terzi od organizzazioni internazionali**;
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 la documentazione delle garanzie adeguate;
f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Questo registro è sicuramente una delle principali novità introdotte con il GDPR e, al contempo, **uno degli adempimenti più importanti concernenti le attività di trattamento**.
Il titolare del trattamento ha, dunque, l'obbligo di documentare la **conformità della propria organizzazione alle prescrizioni della legge**.
Come anticipato, non tutti i soggetti sono tenuti ad istituire il registro delle attività di trattamento. Infatti, l'art. 30 prevede che l'obbligo di istituzione del registro non si applichi alle imprese o **organizzazioni** con meno di 250 dipendenti, **a meno che il trattamento che esse effettuano** possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o **includa il trattamento di categorie particolari** (tra gli altri, i dati relativi alla salute).
Le Associazioni Sportive Dilettantistiche si trovano spesso a trattare dati relativi alla salute (i certificati medici degli atleti) e, pertanto, potrebbero essere tenute ad istituire il registro.
Ad ogni modo, l'istituzione del registro è sempre **consigliata** e valutata positivamente dal Garante per la protezione dei dati personali.

Come conformarsi al GDPR.
Illustrare le operazioni da porre in essere per potersi adeguare al GDPR è un'operazione assolutamente delicata e che andrebbe effettuata caso per caso in base alle specifiche esigenze, finalità, tipologia di dati trattati e di trattamenti che sono effettuati dalla singola Associazione.
Ad ogni modo, in via generale si può suggerire di operare una ricognizione delle misure di sicurezza adottate per la protezione dei dati personali trattati: è necessario, infatti, che i dati siano protetti da accessi non autorizzazioni, dal rischio di perdita, distruzione, manomissione, ecc. A tal proposito, è opportuno archiviare i dati in luoghi protetti da sistemi anti-intrusione: la conservazione cartacea deve avvenire in armadi chiusi a chiave; la conservazione su sistemi informatici deve essere protetta da password, i computer protetti con antivirus e firewall. È possibile adottare ulteriori misure di protezione (indicate anche dal GDPR) come la pseudonimizzazione dei dati o la criptografia. Inoltre, è molto importante effettuare periodicamente la copia di back-up dei dati trattati (al fine di evitare il rischio di perdita, distruzione, ecc.).
Il secondo adempimento molto importante è quello di **aggiornare l'informativa privacy** rendendola conforme alle disposizioni del GDPR. È necessario che il titolare sia in grado di dimostrare di aver reso l'informativa all'interessato.
È opportuno raccogliere il consenso degli interessati, sebbene esistano e siano tutt'ora vigenti le autorizzazioni generali del Garante. Può succedere, infatti, che una specifica finalità di trattamento non sia coperta dall'autorizzazione.
È utile valutare la possibilità di nominare un responsabile del trattamento che collabori con il titolare (a tal fine è necessario, però, stipulare un contratto scritto tra il titolare e il responsabile del trattamento).