

## **“Regolamento europeo in materia di protezione dei dati personali”**

**Dal 25 maggio 2018** è in vigore in tutti i Paesi dell’Unione europea il nuovo **“Regolamento europeo in materia di protezione dei dati personali”** (Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016).

Il nuovo Regolamento, meglio conosciuto come **GDPR** (in inglese “General Data Protection Regulation”) è stato pubblicato nella Gazzetta Ufficiale dell’Unione europea del 4 maggio 2016 ma sono stati concessi oltre due anni di tempo agli Stati UE per allineare la loro normativa a quella europea.

Il Parlamento italiano, con la legge 25 ottobre 2017, n. 163, (Gazzetta ufficiale del 6 novembre 2017), ha allo scopo delegato il Governo, che a seguito di un rinvio, dovrà provvedere entro il 21 agosto 2018.

**Dal 25 maggio 2018, tutti i soggetti che trattano dati personali dovranno adeguarsi alle nuove disposizioni.**

Secondo l’art. 4 del GDPR è considerata **“dato personale”** qualsiasi informazione che renda una persona fisica identificata o identificabile, con particolare riferimento a un dato identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, etc.

**I dati acquisiti dalle asd e o ssd al momento del tesseramento rientrano nell’oggetto della nuova normativa sulla privacy?**

Le associazioni o società sportive che tali dati raccolgono e conservano sia per fini interni sia per trasmetterli alle PGS per il rilascio della tessera hanno pertanto l’obbligo di adeguarsi alla nuova normativa.

### **Il trattamento dei dati**

Dal 25 maggio 2018 **“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 conservazione, l’estrazione, la consultazione, l’uso, la comunicazione etc. mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione.

Si pensi ad operazioni quali archiviazione, elaborazione o anche alla condivisione con terzi tipo invio newsletter, azioni di mailing e messaggistica o app dedicate.

## Quando è lecito trattare i dati?

Il trattamento dei dati è lecito solo **se ricorre almeno una delle condizioni** previste dall'articolo 6 del **GDPR** ossia se:

1. è conseguenza del consenso espresso dall'interessato al trattamento dei propri dati personali per una o più specifiche finalità;
2. oppure se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (si pensi alla stipula della polizza assicurativa o al rilascio della tessera);
3. oppure se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (si pensi all'obbligo di trasmettere al CONI i dati dei soci che praticano attività sportiva nonché dei membri dei Consigli direttivi delle ASD/SSD o all'obbligo statutario di trasmettere alle PGS i dati di tutti i soci).

**E' di norma vietato trattare i dati sensibili**, cioè i dati personali (art. 9) che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, **a meno che il trattamento non sia effettuato nei casi di cui allo stesso articolo 9**, poco frequenti tra le associazioni a noi affiliate (problemi potrebbero esservi con il certificato medico di idoneità sportiva, qualora le associazioni vengano in possesso dei motivi per cui il certificato non può essere rilasciato).

## Il titolare del trattamento dei dati

Il titolare del trattamento dei dati è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati. Egli ha pertanto **ha l'obbligo di mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è conforme alla normativa**.

Possono esservi anche più titolari del trattamento, che determinano in accordo tra loro

## Il DPO

Il Data Protection Officer (DPO) è il termine inglese utilizzato per descrivere il **Responsabile della Protezione dati**.

Questo non può essere descritto come una vera e propria professione (non è collegato a precise abilitazioni), ma come una **funzione indipendente che forma e controlla l'associazione e comunica con l'Autorità Garante e con i singoli interessati**.

**La nomina del DPO** è obbligatoria in una serie di ipotesi previste dall'art. 37 del Regolamento, ad esempio qualora le attività principali del Titolare/Responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali.

## I contenuti dell'informativa da fornire agli interessati al trattamento dei dati

E' obbligatorio fornire informativa agli interessati (nel nostro caso, in primo luogo i nostri soci) e in linea di principio per iscritto, che si stanno trattando i loro dati, e le finalità del trattamento.

Rispetto all'attuale normativa, sono più ampi i contenuti dell'informativa che devono essere forniti, da parte del titolare del trattamento dei dati o del responsabile del trattamento dei dati (cioè della persona fisica o giuridica che tratta i dati per conto del titolare), a tutela dell'esercizio della protezione dei dati.

L'informativa deve essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; si deve poi utilizzare un linguaggio chiaro e semplice, in particolare quando le informazioni sono destinate ai minori.

**I contenuti dell'informativa sono elencati in modo tassativo all'articolo 13 del GDPR.**

In caso di raccolta presso l'interessato di dati che lo riguardano (ad esempio un socio che si iscrive ad un'associazione), il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento (di norma l'Associazione e, per essa, il suo legale rappresentante);
- ove applicabile, l'identità e i dati di contatto del suo rappresentante, che, nel caso, deve essere nominato dal titolare. La nomina di un rappresentante non è obbligatoria; quando c'è, deve però essere disciplinata da uno specifico contratto;
- ove applicabile, i dati di contatto del responsabile della protezione dei dati. La nomina di un responsabile della protezione dei dati è obbligatoria solo in alcuni casi, che analizzeremo in un prossimo intervento, insieme alle altre figure prima specificate;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; (nel nostro caso: per quanto riguarda le finalità, potremmo citare l'organizzazione delle attività statutarie, il rilascio della tessera associativa, la stipula delle polizze assicurative, la fornitura al CONI dei dati degli atleti e dei tecnici tesserati. Per quanto riguarda la base giuridica, per gli sportivi potremmo citare la legge sull'obbligo dell'assicurazione per gli sportivi e la normativa CONI dei dati dei tesserati che praticano attività sportiva);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; (nei casi di cui sopra, di nuovo: PGS, compagnia assicurativa, CONI);
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; (ad esempio: sino a che il socio resta tale);
- 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 che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora sia stato espresso il consenso al trattamento dei dati, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo a un'autorità di controllo: il decreto legislativo in via di emanazione la identifica nel Garante per la protezione dei dati personali;
- 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; (è in genere il nostro caso: se non si forniscono i dati personali, non può essere rilasciata la tessera associativa);
- l'esistenza o meno di un processo decisionale automatizzato, compresa la profilazione, e, nel caso ci sia, se ciò sia necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento (è una eventualità poco frequente per le associazioni).

Nel caso in cui i dati non siano stati ottenuti presso l'interessato (art. 14), è pertanto indispensabile, nell'informativa da fornire all'interessato da parte delle associazioni che ne raccolgono i dati, specificare che essi saranno forniti a PGS per regolamentare il rapporto associativo, che PGS fornirà i dati alla compagnia assicurativa per la liquidazione dei sinistri e la stipula delle eventuali polizze integrative nonché, per i soci che praticano attività sportiva, che PGS fornirà i dati al CONI per gli adempimenti di legge.

## Il consenso al trattamento dei dati.

Il nuovo **GDPR** prescrive esplicitamente che, qualora il trattamento dei dati sia basato sul consenso (art.7) esso debba essere esplicito, anche se non necessariamente in forma scritta, purché inequivocabile e concludente. Se il consenso però è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Non è ammesso il consenso tacito o presunto.

Il consenso dei minori è valido a partire dai 16 anni (il decreto legislativo in corso di approvazione propone 14 anni); prima di tale età il consenso deve essere rilasciato da chi esercita la responsabilità genitoriale.

## Le sanzioni

**In concreto, pertanto, le Associazioni e le Società sportive dilettantistiche, sin da subito, devono verificare il contenuto delle informative rese agli interessati e le modalità di acquisizione del consenso al trattamento e, specialmente se si tratta di minori, e sincerarsi che queste contengano i requisiti minimi previsti dal GDPR; in difetto, è necessario procedere all'adeguamento nel minor tempo possibile.**

Inoltre, stante la precettività di tutte le norme contenute nel Regolamento Europeo ed in attesa di un intervento di adeguamento normativo interno, occorre adottare i modelli di gestione imposti dal GDPR e dotarsi dei meccanismi di controllo delle procedure, al fine di garantire a tutti gli associati tutela e protezione nel trattamento dei dati e di permettere loro, altresì, di esercitare i diritti introdotti dal Regolamento tra i quali, ad esempio, quello previsto dall'art. 20 relativo alla portabilità dei dati, applicabile nei casi di trattamento effettuato con mezzi automatizzati, particolarmente rilevante in caso di trasferimento da un'associazione/società sportiva all'altra.

Il mancato adeguamento alla normativa sancita dal GDPR, "General Data Protection Regulation" – Regolamento UE 2016/679, può comportare rilevanti sanzioni amministrative e penali.

Vengono puniti il mancato rispetto delle regolari procedure di informazione, acquisizione, conservazione, elaborazione, trasmissione e gestione dei dati. In conclusione, anche le Associazioni e le Società sportive, che detengono dati personali e sensibili di dipendenti, soci, volontari, atleti, allenatori e altri, dovranno adeguarsi alle nuove disposizioni facendo un'analisi della propria situazione rispetto ai dati gestiti, individuando le aree di intervento ed attivando le misure tecniche ed organizzative necessarie.

In particolare, per evitare pesanti sanzioni, ciascuna società o associazione sportiva dilettantistica dovrà essere in grado di dimostrare che l'assetto organizzativo prescelto sia adeguato, adottando un modello organizzativo privacy articolato e completo, nel rispetto di quanto statuito dal GDPR.